bitdefender 9

Standard

Benutzerhandbuch

Antivirus

Copyright © 2005 SOFTWIN

BitDefender 9 Standard

Benutzerhandbuch

SOFTWIN

Veröffentlicht 2005.09.16
Build 9.0.1

Copyright © 2005 SOFTWIN

bitdefender
secure your every bit

Inhaltsverzeichnis

Endbenutzer software-lizenzvertrag ..... **ix**

Vorwort ..... **xiii**
1. Verwendete Konventionen xiii
1.1. Typografie xiii
1.2. Symbole xiv
2. Struktur xiv
3. Ihre Mithilfe xv

Installation von BitDefender 1

1. Installation von BitDefender 9 Standard **3**
1.1. Systemanforderungen 3
1.2. Installationsschritte 4
1.3. Upgrade von einer vorherigen Version 6
1.4. Ändern, Reparieren, Deinstallation 7

Beschreibung und Bestandteile 9

2. Überblick **11**
2.1. Warum BitDefender? 11
2.2. Data Security Division 13
2.3. SOFTWIN 13

3. BitDefender 9 Standard **15**
3.1. Antivirus 15
3.2. Erweiterte Funktionen 16

4. Die BitDefender Module **17**
4.1. Das Modul Allgemein 17
4.2. Das Modul Antivirus 17
4.3. Das Modul Update 18

Die Management Konsole 19

5. Überblick **21**
5.1. System Ablage 22
5.2. Scan Aktionsbalken 23

6. Das Modul Allgemein **25**

6.1. Status aller BitDefender Module 25
6.1.1. Virus Schild 26
6.1.2. Automatisches Update 27
6.2. Registrierung des Produkts 27
6.3. Allgemeine Einstellungen 29
6.4. Ereignisanzeige 32
6.5. Info über 34

7. Das Modul Antivirus 37
7.1. Bei Zugriff scannen 37
7.1.1. Wichtigsten Einstellungen 38
7.1.2. Anderer Optionen 39
7.2. Nach Aufforderung prüfen 42
7.2.1. Sofortiges prüfen 44
7.2.2. Scannen mit dem Kontextmenü 52
7.2.3. Prüfen per Drag & Drop 52
7.2.4. Prüfen mit dem BitDefender Planer 54
7.3. Quarantäne 64
7.4. Berichte 68

8. Das Modul Update 71
8.1. Das automatische Update 71
8.2. Das manuelle Update 73
8.2.1. Das manuelle Update mit der `weekly.exe` Datei 73
8.2.2. Das manuelle Update per `ZIP Archiv` 74
8.3. Update-Einstellungen 76
8.3.1. Update-Adresse 77
8.3.2. Automatisches Update 78
8.3.3. Update-Bestätigung beim manuellen Update 78
8.3.4. Erweiterte Einstellungen 79

Tipps und Tricks 81

9. Tipps und Tricks 83
9.1. Antivirus 83

BitDefender Notfall CD 85

10. Übersicht 87
10.1. Was ist Knoppix? 87
10.2. Systemanforderungen 87
10.3. Integrierte Software 88
10.4. BitDefender Lösungen auf dieser CD-ROM 89
10.4.1. BitDefender SMTP Proxy 89
10.4.2. BitDefender Remote Admin 89
10.4.3. BitDefender Linux Edition 90

11. LinuxDefender Kurzanleitung 91
11.1. Starten und Beenden 91
11.1.1. LinuxDefender starten 91
11.1.2. LinuxDefender beenden 94
11.2. Internetverbindung konfigurieren 95
11.3. BitDefender per Update aktualisieren 95
11.4. Prüfvorgänge durchführen 96
11.4.1. Wie erhalte ich Zugriff auf meine Daten unter Windows? 96
11.4.2. Wie führe ich einen Prüfvorgang durch? 97
11.5. Erstellen einer Ad-Hoc Mail-Filterungs-Lösung 98
11.5.1. Vorbereitende Maßnahmen 98
11.5.2. Der Mail-Filter 99
11.6. Eine Netzwerk-Sicherheitsprüfung durchführen 100
11.6.1. Auf Rootkits überprüfen 100
11.6.2. Nessus – der Netzwerk Scanner 101
11.7. Den RAM Ihres Computers überprüfen 101

Getting help 103

12. Support 105
12.1. Technische Beratung 105
12.2. Online-Hilfe 105
12.2.1. BitDefender Knowledge Base 105
12.3. Kontaktinformationen 106
12.3.1. Kontaktadressen 106
12.3.2. Adresse 106

13. Häufig gestellte Fragen 109

Wörterbuch 111

Endbenutzer software-lizenzvertrag

Der Lizenzvertrag und die Gewährleistungsbestimmungen sind ein rechtsgültiger Vertrag zwischen Ihnen (einer natürlichen oder juristischen Person, im folgenden Benutzer genannt) und der SOFTWIN zur Benutzung des oben und folgend genannten SOFTWIN SOFTWAREPRODUKTES, welches außer dem eigentlichen SOFTWARE-PRODUKT auch dazugehörige Medien, gedruckte Materialien und die Nutzung von Online- und underen Medien beinhaltet. Das SOFTWAREPRODUKT und die zugehörigen Materialien sind durch US-amerikanische Urheberrechtsgesetze und internationale Urheberrechtsverträge geschützt. Indem Sie das SOFTWAREPRODUKT installieren, kopieren, downloaden, darauf zugreifen oder es underweitig verwenden, erklären Sie sich damit einverstunden, durch die Bestimmungen des Lizenzvertrages und der Gewährleistungsbestimmungen gebunden zu sein. Falls Sie den Bestimmungen dieses Lizenzvertrages und der Gewährleistungsbestimmungen nicht zustimmen, ist der Hersteller SOFTWIN nicht bereit, das SOFTWAREPRODUKT an Sie zu lizenzieren. In diesem Falle sind Sie nicht berechtigt, das SOFTWAREPRODUKT zu verwenden oder zu kopieren. Die Rückgabe des Produktes kann nur innerhalb von 30 Tagen nach dem Kauf beim der Verkäufer des SOFTWAREPRODUKTS unter voller Rückerstattung des Kaufpreises erfolgen. Eine rechtsgültiger Kaufbeleg ist dazu erforderlich.

Das SOFTWAREPRODUKT ist durch Urheberrechtsgesetze und internationale Urheberrechtsverträge genauso geschützt, wie durch undere Gesetze und Verträge zum Schutz des geistigen Eigentums. Das SOFTWAREPRODUKT wird an Sie lizenziert, nicht verkauft.

LIZENZEINRÄUMUNG. Dieser Vertrag gewährt Ihnen und nur Ihnen eine nicht ausschließliche Lizenz. Folgende Rechte werden Ihnen eingeräumt:

ANWENDUNGSSOFTWARE. Der Benutzer darf eine Kopie des SOFTWAREPRODUKTES auf einem Betriebssystem und einen Einzelplatzrechner installieren und benutzen. Der Benutzer, auf dessen Einzelplatzrechner das SOFTWAREPRODUKT installiert ist, darf eine weitere (zweite Kopie) zu seiner eigenen Benutzung auf einem tragbaren Rechner installieren.

NETZWERKBENUTZUNG. Der Benutzer darf eine Kopie des SOFTWAREPRODUKTES auf einem Speicherplatz innerhalb eines geschlossenen Netzwerkes speichern und

installieren, um es von dort wiederum für einen Einzelplatzrechner zu nutzen. Für jeden weiteren Einzelplatzrechner auf dem eine Kopie des SOFTWAREPRODUKTES installiert ist oder gestartet wird, muss der Benutzer eine weitere Lizenz erwerben und ausweisen. Eine einzelne Lizenz des SOFTWAREPRODUKTES darf nicht auf mehreren Einzelplatzrechnern oder gleichzeitig auf verschiedenen Rechnern genutzt werden. Falls der Benutzer eine mehrfache oder gleichzeitige Nutzung des SOFTWAREPRODUKTES wünscht, empfiehlt SOFTWIN den Erwerb einer Multilizenz.

MULTILIZENZ. Falls der Benutzer eine Multilizenz des SOFTWAREPRODUKTES erworben hat und diesen Lizenzvertrag dazu erhalten hat, darf er so viele Kopien installieren und benutzen wie unter "Lizenzierte Kopien" angegeben ist. Der Benutzer darf zusätzlich dieselbe Anzahl an Kopien auf tragbaren Rechnern installieren und diese nach denselben Regeln wie unter Anwendungssoftware beschrieben (also nicht gleichzeitig) nutzen.

LIZENZGÜLTIGKEIT. Der Lizenzvertrag über das SOFTWAREPRODUKT beginnt mit dem Tag der Installation, der Speicherung oder undererseits mit dem Tag der ersten Benutzung und behält seine Gültigkeit auf dem Einzelplatzrechner, auf dem es ursprünglich (zu erst) installiert wurde.

UPGRADES. Sollte das SOFTWAREPRODUKT mit der Bezeichnung Upgrade gekennzeichnet sein, muss der Benutzer für eine berechtigte Nutzung ein gültiges, von SOFTWIN als berechtigtes anerkanntes, underes SOFTWAREPRODUKT lizenziert haben. Das als Upgrade gekennzeichnete SOFTWAREPRODUKT ersetzt und / oder ergänzt das zum Upgrade berechtigende SOFTWAREPRODUKT. Der Benutzer darf das aus dem Upgrade resultierende SOFTWAREPRODUKT nur nach dem hier vorliegenden Lizenzvertrag nutzen. Sollte das als Upgrade gekennzeichnete SOFTWAREPRODUKT ein Upgrade für eine einzelne Komponente eines kompletten Softwarepaketes sein, darf das SOFTWAREPRODUKT auch nur als einzelner Bestundteil dieses Softwarepaketes genutzt und transferiert werden und darf nicht als separates Produkt auf mehr als einem Einzelplatzrechner genutzt werden.

URHEBERRECHT. Alle Rechte und geistigen Eigentumsrechte an dem SOFTWAREPRODUKT (einschließlich, aber nicht beschränkt auf Logos, Bilder, Fotografien, Animationen, Video, Audio, Musik, Text und "Applets", die in dem SOFTWAREPRODUKT enthalten sind), den gedruckten Begleitmaterialien und jeder Kopie des SOFTWAREPRODUKTS liegen bei SOFTWIN. Das SOFTWAREPRODUKT ist durch anwendbare Urheberrechtsgesetze und undere Gesetze und Vereinbarungen über geistiges Eigentum geschützt. Darum muss der Benutzer das SOFTWAREPRODUKT wie jedes undere urheberrechtliche Produkt behundeln, mit der Ausnahme, dass er das SOFTWAREPRODUKT auf einem Einzelplatzrechner installieren darf und das Original zu

Sicherungszwecken speichern darf. Der Benutzer darf die zugehörigen, gedruckten Materialien nicht vervielfältigen. Der Benutzer muss das SOFTWAREPRODUKT als Ganzes, wie erhalten, inklusiver aller Urheberrechtsvermerke und aller zugehörigen Materialien und Medien in der ihm vorliegenden Form bewahren. Der Benutzer ist nicht berechtigt, das SOFTWAREPRODUKT weiter zu lizenzieren, zu vermieten, zu verleihen und / oder zu verkaufen. Der Benutzer darf das SOFTWAREPRODUKT nicht zurückentwickeln (Reverse Engineering), dekompilieren, disassemblieren, daraus Derivate erzeugen, modifizieren, übersetzen oder irgendeinen underen Versuch starten, den Quellcode des SOFTWAREPRODUKTES freizulegen.

EINGESCHRÄNKTE GEWÄHRLEISTUNG. SOFTWIN gewährleistet für einen Zeitraum von 30 Tagen, dass das Medium auf dem das SOFTWAREPRODUKT geliefert wird, frei von allen Defekten ist. Sollte dies nicht der Fall sein, wird SOFTWIN das Medium austauschen oder dem Benutzer den Betrag zurück erstatten, den der Benutzer für das SOFTWAREPRODUKT bezahlt hat. SOFTWIN gewährleistet weder die dauerhafte Verfügbarkeit, noch die Fehlerfreiheit des SOFTWAREPRODUKTES, noch dass Unzulänglichkeiten und Fehler des SOFTWAREPRODUKTES behoben werden. SOFTWIN gewährleistet ebenso nicht, dass das SOFTWAREPRODUKT den Anforderungen des Benutzers entspricht. SOFTWIN übernimmt ausdrücklich keinerlei Garantie jeder Art, ausdrücklich oder stillschweigend, einschließlich, jedoch nicht beschränkt auf die stillschweigenden Garantien der Eignung zum Verkauf, oder zu einem bestimmten Zweck, oder die Nichtverletzung von Rechten Dritter. Der Benutzer trägt das alleinige Risiko für die Verwendung und Leistung des SOFTWAREPRODUKTES. Diese Gewährleitung gibt dem Benutzer bestimmte Rechte, die von Lund zu Lund verschieden sein können.

BESCHRÄNKUNG DER HAFTUNG. Jeder Benutzer des SOFTWAREPRODUKTES, der dieses benutzt, testet oder auch nur ausprobiert trägt alleinig das Risiko, das aus der Qualität und Performance des SOFTWAREPRODUKTES entsteht. In keinem Fall können SOFTWIN oder ihre Lieferanten auf irgendeine Weise für, durch Verwendung des SOFTWAREPRODUKTES, entstundene Schäden jeder Art haftbar gemacht werden, einschließlich und ohne Beschränkung, direkter und indirekter, zufälliger und spezieller Schäden die aus der Verwendung, Performance oder der Verfügbarmachung des SOFTWAREPRODUKTES entstunden sind. Dies gilt auch dann, wenn SOFTWIN über existierende und / oder mögliche Schäden informiert wurde. IN KEINEM FALL KÖNNEN SCHADENSERSATZANSPRÜCHE IN EINER HÖHE GELTEND GEMACHT WERDEN, DIE DEN KAUFPREIS DES SOFTWAREPRODUKTES ÜBERSTEIGEN. Alle Erklärungen und Beschränkungen behalten auf jeden Fall ihre Gültigkeit unabhängig von der Nutzungsart (reguläre Benutzung, Test, etc.).

WICHTIGE INFORMATION FÜR DEN BENUTZER. DIESES SOFTWAREPRODUKT IST NICHT FEHLERTOLERANT UND IST AUCH NICHT FÜR EINE NUTZUNG IN KRITISCHEN UMGEBUNGEN, IN DENEN ES AUF EINE AUSFALLSICHERE PERFORMANCE UND BEDIENUNG ANKOMMT, KONZIPIERT UND ERSTELLT. DIESES SOFTWAREPRODUKT IST NICHT GEEIGNET ZUR NUTZUNG IM LUFTVERKEHR, IN NUKLEARKRAFTWERKEN, IN KOMMUNIKATIONSSYSTEMEN, IN WAFFENSYSTEMEN, IN DIREKTEN ODER INDIREKTEN LEBENSERHALTUNGSSYSTEMEN ODER IRGENDEINEM ANDEREN SYSTEM, DESSEN AUSFALL ZU TODESFÄLLEN, KÖRPERLICHEN SCHÄDEN ODER VERMÖGENSSCHÄDEN FÜHREN KÖNNTE.

REGIERUNGSBEGRENZUNGESRECHTE/ BEGRENZUNGSRECHTERKLÄRUNG. Benutzung, Vervielfältigung, Offenbarung durch die Regierung unterliegen den Einschränkungen, die in folgenden Subparagraphen festgesetzt sind: (c)(1)(ii) Rechte hinsichtlich der Technischen Daten und Computer Software DFARS 252.227-7013 oder den Subparagraphen (c)(1) und (2) der Anwendung der Klausel der begrenzten Rechte der Kommerziellen Computersoftware 48 CFR 52.227-19. Kontaktieren Sie SOFTWIN, Fabrica de Glucoza Str.5, 72322-Sect.2, Bukarest, Rumänien, Tel. 0040-21-2330780 oder Fax:0040-21-2330763.

ALLGEMEIN. Dieser Vertrag unterliegt dem Recht von Rumänien. Diese Vereinbarung darf nur durch eine Ergänzung zum Lizenzvertrag und der Gewährleistungsbestimmung verändert werden. Diese Änderung muss in schriftlicher Form erfolgen und muss von SOFTWIN und dem Benutzer unterzeichnet sein. Dieser Vertrag wurde in deutscher Sprache geschrieben und kann nicht in eine undere Sprache übersetzt oder interpretiert werden. Preise, Kosten und Gebühren, in Zusammenhang mit der Benutzung des SOFTWAREPRODUKTES können ohne weitere Ankündigung geändert werden. Ist oder wird eine Bestimmung dieses Vertrages wegen Verstoßes gegen zwingende gesetzliche Bestimmungen unwirksam oder wird sie für unwirksam erklärt, so wird hierdurch die Gültigkeit des übrigen, mit der unwirksamen Bestimmung nicht unmittelbar zusammenhängenden Vertragsteils, nicht berührt. BitDefender und alle zugehörigen Logos sind eingetragene Titel und Marken von SOFTWIN. Alle underen Marken und Titel sind Eigentum der jeweiligen Rechteinhaber.

Vorwort

Dieses Benutzerhandbuch ist für alle Benutzer die sich für BitDefender 9 Standard als Sicherheitslösung entschieden haben vorgesehen. Die in diesem Dokument beschriebenen Informationen sind nicht nur für IT-Profis gedacht, sondern auch für all diejenigen die sich nur in Ihrer Freizeit mit dem Computer beschäftigen.

Es wird beschrieben wie BitDefender 9 Standard zu handhaben ist, wie das Produkt optimal konfiguriert werden kann und wie Sie die Einstellungen Ihren Bedürfnissen anpassen können. So lernen Sie optimal mit diesem Produkt umzugehen und es effektiv einzusetzen.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

1. Verwendete Konventionen

1.1. Typografie

Um die Lesbarkeit zu fördern werden verschiedene Arten von Textstilen verwendet. Die jeweiligen Bedeutungen entnehmen Sie bitte der Tabelle unterhalb.

Erscheinungsbild	Beschreibung
`Syntaxbeispiele`	Syntaxbeispiele werden in einer Schriftart mit `fester Laufweite` angegeben.
http://www.bitdefender.com	Verweise (Links) auf externe Inhalte wie z.B. Web-Seiten oder FTP-Server.
<support@bitdefender.com>	Verweise auf E-Mail-Adressen, z.B. zur Kontakt-aufnahme.

Erscheinungsbild	Beschreibung
Vorwort [xiii]	Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.
`Dateiname`	Dateien und Verzeichnisse werden in einer Schriftart mit `fester Laufweite` angegeben.
Optionen	Optionen wie z.B. Schaltflächen oder Checkbox-Elemente werden in **fett gedruckt** angegeben.
`Beispielquelltext`	Beispielquelltexte werden in einer Schriftart mit fester Laufweite angegeben.

1.2. Symbole

Bei diesen Symbolen handelt es sich um Hinweise innerhalb des Textflusses welche mit einer kleinen Grafik markiert sind. Hierbei handelt es sich um Informationen die Sie in jedem Fall beachten sollten.

Anmerkung

Diese Bemerkung dient lediglich zur Überprüfung. Notizen erhalten nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.

Wichtig

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden signifikante Informationen zum jeweiligen Thema bereitgestellt. Es wird nicht empfohlen diese zu übergehen.

Warnung

Diese kritische Information sollten Sie mit höchster Aufmerksamkeit verfolgen. Hier angegebenen Anweisungen und Informationen sollten Sie auf jeden Fall Beachtung schenken. Sie sollten diese Informationen sorgsam lesen und verstanden haben, da es sich um eine höchst prekäre Thematik handelt.

2. Struktur

Dieses Handbuch ist in fünf Abschnitte unterteilt, welche die folgenden Hauptthemen beinhalten: Beschreibung und Funktionen, Installation, Konfiguration, Verwendung und Hilfe erhalten. Des Weiteren beinhaltet dieses Dokument einen Glossar und

Anhänge um den ein oder anderen Aspekt zu klären der sonst ggf. zu technischen Problemen führen könnte.

Beschreibung und Funktionen. Eine kurze Einführung in BitDefender welche erklärt was BitDefender genau ist und welches Unternehmen dahinter steht. Sie erhalten eine Einführung in BitDefender 9 Standard, die Funktionen dieses Produkts und Details zu den einzelnen Modulen.

Installation. Schritt-für-Schritt Anleitung zur Installation von BitDefender auf Ihrem Computer. Hierbei erhalten Sie ausführliche Informationen für eine erfolgreiche Installation von BitDefender 9 Standard und werden durch jeden Schritt begleitet. Zusätzlich wird beschreiben wie eine Deinstallation von BitDefender durchzuführen ist.

Konfiguration. Beschreibt die einfache Verwaltung und Konfiguration von BitDefender. Dieser Abschnitt erklärt wie das BitDefender 9 Standard zu registrieren ist, wie ein Prüfvorgang durchgeführt werden kann und wie ein Update von BitDefender durchgeführt werden kann.

Hilfe erhalten. Beschreibt wie Sie Hilfe bzw. Unterstützung zu dem Produkt erhalten und erhält zusätzlich eine Liste mit den an häufigsten gestellten Fragen (FAQ).

Empfohlene Vorgehensweisen. Folgen Sie den hier beschriebenen Anweisungen um Ihren Computer bestmöglich zu schützen und in Zukunft frei von Viren zu halten.

Glossar. Im Glossar werden technische Ausdrücke und seltene Bezeichnungen die in diesem Dokument zu finden sind erklärt.

3. Ihre Mithilfe

Wir laden Sie dazu ein uns bei der Verbesserung dieses Dokuments mitzuhelfen. Wir haben sämtliche Informationen in diesem Dokument bestmöglich überprüft um somit die Qualität sicherzustellen.

Falls Sie dennoch Fehler finden, so teilen Sie uns diese bitte mit indem Sie uns per E-Mail unter der Adresse <documentation@bitdefender.com> kontaktieren.

Anmerkung

Bitte schreiben Sie Ihre Verbesserungsvorschläge in Englisch, da diese andernfalls leider nicht beachtet werden können.

Installation von BitDefender

Kapitel 1. Installation von BitDefender 9 Standard

Der Abschnitt **Installation von BitDefender 9 Standard** beschreibt die folgenden Themen:

- Systemanforderungen
- Installationsschritte
- Upgrade von einer vorherigen Version
- Ändern, Reparieren, Deinstallation

1.1. Systemanforderungen

Um eine korrekte Funktion des Produkts sicherzustellen überprüfen Sie bitte zunächst ob Ihr Computer die folgenden Systemanforderungen erfüllt:

- **Minimum Prozessor** - Pentium MMX 200 MHz
- **Minimum Festplattenspeicher** - 40MB
- **Minimum RAM Speicher** - 64MB (128MB empfohlen)
- **Betriebssystem** - Windows 98/NT-SP6/ME/2000/XP; Internet Explorer 4.0 (oder höher)

Warnung

BitDefender 9 Standard kann nicht auf den folgenden Betriebssystemen installiert werden: Windows NT 4.0 Server, Windows 2000 Server und Windows 2003 Server. Für diese Plattformen bieten wir gesonderte Lösungen an die speziell für Fileserver, E-Mail-Server und Gateway-Server ausgelegt sind.

1.2. Installationsschritte

Klicken Sie mit einem Doppelklick auf den Setup Ordner. Dieses startet den Setupassistenten, der Ihnen bei der Installation hilft:

Installationsschritte:

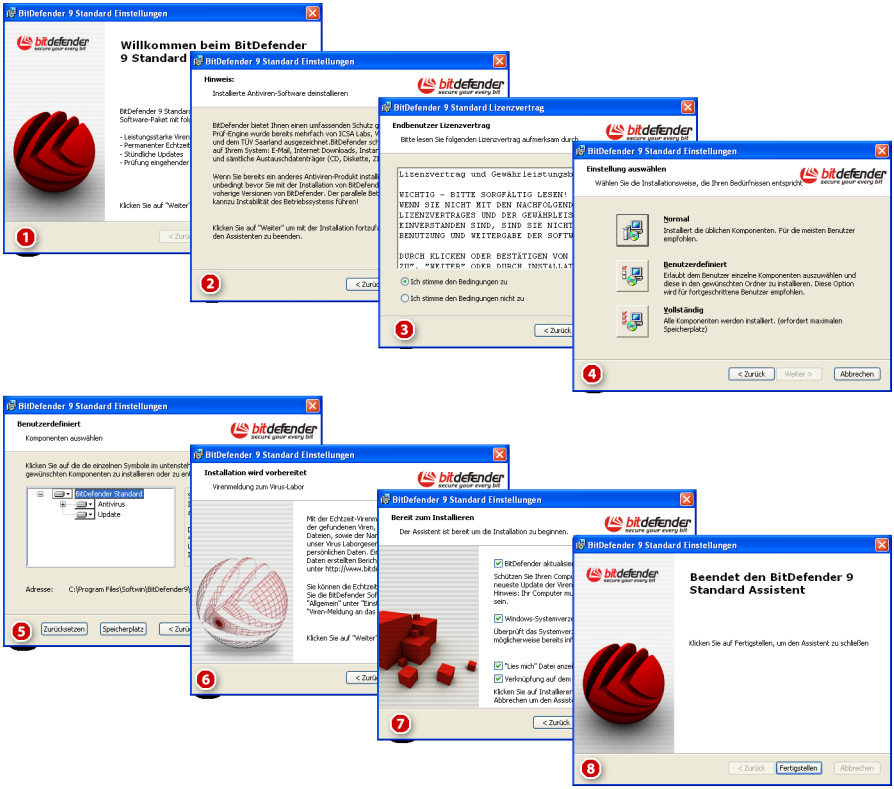


Abbildung 1.1. Installationsschritte

1. Klicken Sie auf **Weiter** um fortzufahren, oder auf **Abbrechen**, um die Installation zu beenden.

2. Klicken Sie auf **Weiter** um fortzufahren, oder auf **Zurück** um wieder zum ersten Schritt zu kommen.

3. Bitte lessen Sie die Lizenzvereinbarung, wählen Sie **Ich stimme den Bedingungen zu** und dann auf **Weiter**. Wenn Sie den Bedingungen nicht zustimmen, klicken Sie auf **Abbrechen**. Die Installation wird abgebrochen und Sie verlassen das Setup.

4. Sie können bei der Installation zwischen verschieden Arten wählen: Normal, Benutzerdefiniert oder Vollständig.

   - **Normal** - Das Programm wird mit den gebräuchlisten Einstellungen installiert. Diese Einstellung ist die empfohlenste für die meisten Nutzer.
   - **Benutzerdefiniert** - Sie können die Einstellungen wählen, welche Sie installieren wollen. Diese Option ist für fortgeschrittene Nutzer empfohlen.
   - **Vollständig** - Alle Komponenten des Programms werden installiert.

   Wenn Sie **Normal** oder **Vollständig** gewählt haben, überspringen Sie Schritt 5

5. Wenn Sie **Benutzerdefiniert** gewählt haben, öffnet sich ein Fenster mit allen BitDefender Komponenten, so dass Sie aus einer Liste wählen können, was Sie installieren möchten.

   Wenn Sie auf eine Komponente klicken, erscheint eine kurze Beschreibung (inbegriffen das Minimum an Festplattenspeicher). Wenn Sie auf ein symbol klicken erscheint ein neues Fenster und Sie können auswählen, welche Komponente Sie installieren wollen.

   Sie können den Ordner wählen, in welchem das Produkt installiert werden soll. Standardmäßig wird BitDefender im Ordner `C:\Program Files\Softwin\BitDefender 9` installiert.

   Falls Sie einen anderen Ordner wählen wollen, klicken Sie auf **Durchsuchen** und ein neues Fenster wird geöffnet, wo Sie einen neuen Ordner wählen können. Klicken Sie auf **Weiter**.

6. Klicken Sie auf **Weiter**.

7. Sie haben vier Möglichkeiten:

- **Update BitDefender** - um BitDefender nach der Installation upzudaten. Ihr System muss mit dem Internet verbunden sein.
- **Durchführen eines kompletten Scans** - um einen kompletten Virenscan auf Ihrem Computer nach dem Ende der Installation durchzuführen.
- **Öffnen der Readme Datei** - öffnen der Readme Datei am Ende der Installation.
- **Speichern eines Symbols auf Ihrem Desktop** - um ein Symbol am Ende der Installation auf Ihrem Desktop zu speichern.

Klicken Sie auf **Installieren**, um mit der Installation zu beginnen.

8. Klicken Sie auf **Fertigstellen**, um die Installation abzuschließen. Wenn Sie die standardmäßigen Einstellungen für die Installation akzeptiert haben, wurde ein neuer Ordner mit dem Namen `Softwin` in `Programme Dateien` angelegt, der den Unterordner `BitDefender 9` beinhaltet.

Anmerkung

Sie werden aufgefordert, Ihren Computer neu zu starten, damit der Setupassistent das Setup beenden kann.

1.3. Upgrade von einer vorherigen Version

Die Prozedur für das Upgrade kann über zwei Schritte erfolgen:

- Installation ohne die Vorgängerversion zu deinstallieren – nur beim Upgrade von v8 auf v9

  Doppelklick auf die Setup – Datei und folgen Sie bitte dem Assistenten wie beschrieben im Abschnitt *„Installationsschritte“* (S. 4).

Wichtig

Während des Installationsprozesses erscheint eine Fehleranzeige beruhend auf dem `FILESpy-Dienst`, will appear. Bitte klicken Sie auf **OK**, um mit der Installation fortzufahren.

- Deinstallieren Sie bitte die Vorgängerversion und installieren Sie die neue Version- Dies gilt für alle BitDefender Versionen

  Zunächst deinstallieren Sie die Vorgängerversion. Starten Sie dann den Computer neu und installieren Sie die neue Version wie beschrieben in Abschnitt *„Installationsschritte“* (S. 4).

Wichtig

Falls Sie von der Version 8 auf die Version 9 aufrüsten empfehlen wir Ihnen, die BitDefender-Einstellungen zu speichern. Nachdem der Upgrade-Vorgang abgeschlossen ist, können Sie die gespeicherten Einstellungen wieder laden.

1.4. Ändern, Reparieren, Deinstallation

Wenn Sie BitDefender 9 Standard modifizieren, reparieren oder entfernen wollen, folgen Sie dem Windows Start Menü: **Start** -> **Programme** -> **BitDefender 9** -> **Ändern, Reparieren, Deinstallation**.

Sie werden aufgefordert, Ihre Eingabe zu bestätigen mit einem klick auf **Weiter**. Ein Neues Fenster öffnet sich und Sie können wählen zwischen:

- **Ändern** - Auswahl neuer Programmkomponenten oder bereits installierter Komponenten;
- **Reparieren** - erneute Installation aller Komponenten;

Wichtig

Wir empfehlen Ihnen, vor der Instandsetzung des Produktes die BitDefender – Basiseinstellungen zu speichern. Nach dem Instandsetzungssvorgang können alle Einstellungen wieder geladen werden.

- **Deinstallation** - entfernt alle installierten Komponenten.

Um mit dem Setup fortzufahren, wählen Sie bitte eine dieser aufgeführten Optionen. Wir empfehlen **Deinstallation** für eine saubere Installation. Nach dem Deinstallieren löschen Sie am besten den Ordner `Softwin` aus dem Ordner `Programme`.

Beschreibung und Bestandteile

Kapitel 2. Überblick

BitDefender stellt Sicherheits-Lösungen bereit die den heutigen Anforderungen an sichere Computersysteme gerecht werden. Mit über 41 Millionen Privat- und Unternehmenskunden in mehr als 100 verschiedenen Ländern ist BitDefender eine der meist genutzten Sicherheitslösungen weltweit.

Die BitDefender -Lösungen umfassen neben dem reinen Schutz vor Viren, Würmern und Trojanern ebenfalls den Schutz vor unerwünschten Spam E-Mails mittels Antispam und vor unerwünschten Eindringlingen über eine Firewall bis hin zu Security Management Solutions und der Beratung bei Erstellung von Sicherheitsrichtlinien für Unternehmensnetzwerke.

BitDefender Professional war weltweit das dritte Produkt seiner Art welches eine ICSA-Zertifizierung für Windows XP erreichte und das erste Produkt welches für seine wegweisenden Innovationen von der Europäischen Kommission ausgezeichnet wurde. Die BitDefender Antivirus-Engine wurde von unabhängigen Instituten weltweit ausgezeichnet, darunter - ICSA Labs, CheckMark, CheckVir, TÜV Saarland und Virus Bulletin.

Hauptsitz von BitDefender ist Bukarest, Rumänien und ist weltweit mit Niederlassungen in Tettnang, Deutschland; Barcelona, Spanien; und Florida, USA vertreten. Website: http://www.bitdefender.com

2.1. Warum BitDefender?

Bewährt: Der Reaktionsfähigste Hersteller von Antiviren-Produkten. Die Reaktionsfähigkeit von BitDefender wurde bereits bei den Ausbrüchen von CodeRed, Nimda, Sircam und auch Badtrans.B und weiteren Schädlingen auf die Probe gestellt. BitDefender war das erste Antiviren-Produkt welches effektive Gegenmittel, sog. „Removal Tools“ für die genannten Schädlinge bereitstellte – und dies vollkommen kostenlos und für Benutzer auf der ganzen Welt. Mit der kontinuierlichen Verbreitung immer neuer Schädlinge und Varianten gehört der effiziente Schutz vor solchen Bedrohungen

mittlerweile zu einem „Must have“ für diejenigen die tagtäglich mit Computersystemen arbeiten.

Innovation: Ausgezeichnet von der Europäischen Kommission und EuroCase. BitDefender wurde zum Gewinner des Europäischen IST-Prize gekürt, welcher von der Europäischen Kommission und Vertreten von 18 Akademien in ganz Europa vergeben wird. Seit acht Jahren vergeben zählt der IST-Prize mittlerweile als Auszeichnung für wegweisende Innovationen und repräsentiert somit die beste Innovation der Europäischen Informationstechnologie.

Umfassend: Sichert Einstiegspunkte im Netzwerk und bietet effektiven Schutz. Sicherheitslösungen mit BitDefender werden den Anforderungen in Unternehmensnetzwerken mehr als gerecht indem sowohl kleine, über mittelständische, bis hin zu Multi-Plattform Netzwerken in weltweit agierenden Konzernen effektiv durch BitDefender-Produkte geschützt werden. Somit wird sichergestellt das Viren und andere Schädlinge erst gar keine Möglichkeit erhalten sich in diesen zu verbreiten.

Optimaler Schutz: Sicherheit vor Bedrohungen auf Ihrem Computer. Da Virenerkennung basierend auf Quellcode-Analyse längst nicht mehr ausreicht um Schädlinge ausreichend früh zu erkennen arbeitet das Team von BitDefender stets an neuen Technologien zur frühzeitigen Erkennung von Schädlingen und pro-aktivem Schutz vor diesen. Eine dieser Technologien ist MIDAS (Malware Intrusion Detection Advanced System) welches über drei Ebenen verteilt arbeitet und somit den pro-aktiven Schutz vor neuen Schädlingen wie Viren, Würmern und Trojanern bietet.

Sicherheitsprodukte wurden geschaffen um in Firmen, Einrichtungen und bei Privatpersonen die folgenden **möglichen Schäden** zu verhindern:

- Wurm-Angriffe
- Störung der Kommunikation durch infizierte E-Mails
- Zusammenbrechen von Servern
- Desinfizierung und Wiederherstellung von Computersystemen
- Produktivitätsverlust durch nicht verfügbare Systeme
- Cracking und unautorisierte Zugriffe auf sensible Daten

Durch die stetige Weiterentwicklung und den pro-aktiven Schutz von BitDefender können die folgenden **Vorteile** gesichert werden:

- Verbesserte Netzwerkverfügbarkeit durch rechtzeitige Unterbindung von Wurm-Angriffen.
- Schutz der Remote-Benutzer und Clients vor Viren-Angriffen.

- Minimierung des Administrativen Aufwands und Kosten durch Remote-Management Funktionalität der BitDefender-Produkte.
- Unterbindung der Verbreitung von Viren und anderen Schädlingen durch den Schutz der zentralen Kommunikationswege wie Fileserver, E-Mail-Server und Gateways mittels BitDefender.

2.2. Data Security Division

SOFTWIN's Data Security Division schaffte es in der Vergangenheit bereits mehrfach die Aufmerksamkeit auf sich zu ziehen. So unter anderem mit dem ersten intelligenten Update ohne Eingriff durch den Benutzer, Remote-Verwaltung von Antiviren-Produkten durch WAP-Technologie oder die erste Personal Firewall welche direkt in ein Antiviren-Produkt integriert war.

Sicherheitslösungen mit der Data Security Division werden den Anforderungen in Firmennetzwerken mehr als gerecht indem sowohl kleine, über mittelständische, bis hin zu Multi-Plattform Netzwerken in weltweit agierenden Konzernen effektiv durch BitDefender-Produkte geschützt werden. Somit wird sichergestellt das Viren und andere Schädlinge erst gar keine Möglichkeit erhalten sich in diesen zu verbreiten.

2.3. SOFTWIN

Mit dem Hauptsitz in Bukarest ist SOFTWIN der führende Anbieter von Sicherheits-Lösungen und -Diensten in Rumänien.

SOFTWIN hat es sich zur Aufgabe gemacht Sicherheits-Lösungen und -Dienste bereitzustellen die den heutigen Anforderungen von schnell expandieren Firmen im Bereich IT-Sicherheit entsprechen und diesen Vorsprung auszubauen.

SOFTWIN erreicht durch die Übernahme von Outsourcing-Aktivitäten, dass sich Firmen wieder auf Ihre eigentlichen Geschäftsfelder konzentrieren und dennoch auf neue Märkte expandieren können.

SOFTWIN beschäftigt weltweit über 500 qualifizierte Mitarbeiter die erfahren in der Entwicklung, der Anpassung von Lösungen für Kunden und im Service-Bereich sind.

SOFTWIN hat seit der Gründung im Jahre 1990 den durchschnittlich erwirtschafteten Ertrag um mehr als 30% gesteigert.

SOFTWIN ist in vier Divisionen unterteilt, welche sich nach den Hauptgeschäftsfeldern des Unternehmens richten:

- CRM
- Business Information Solutions
- eContent Solutions
- Data Security Solutions

SOFTWIN stellt Kunden weltweit Dienste und Lösungen zur Verfügung. Über 90% des Absatzes wird mit dem Export von Diensten und Lösungen in die Europäische Union und die Vereinigten Staaten von Amerika erwirtschaftet.

Unter Verwendung innovativer und topaktueller Technologien hat SOFTWIN bereits mehr als 500 Software-Entwicklungs-Projekte und über 3.500 Content-Structuring-Projekte für Kunden im Internationalen Umfeld entwickelt. Über 43 Millionen Kunden in 80 verschiedenen Ländern vertrauen auf Produkte und Lösungen von SOFTWIN's Data Security Division. Es wurden mehr als 1,5 Millionen Anrufe über Call-Center-Projekte der CRM Division angenommen.

Kapitel 3. BitDefender 9 Standard

Die **BitDefender 9 Standard** ist mehr als "nur" als eine AntiViren Lösung. Die Such- und Reparaturengine der **BitDefender 9 Standard** ist durch die ICSA Labs, dusch Chekmark,Virus Bulletin, Checkvir und TÜV zertifiziert.

3.1. Antivirus

Die Aufgabe des Antivirus-Moduls ist sicherzustellen, dass alle Viren entdeckt und beseitigt werden. BitDefender nutzt robuste Scan-Maschinen, die von ICSA Labs, Virus Bulletin, Checkmark, Checkvir und TÜV zertifiziert worden sind.

Heuristik in virtueller Umgebung. Die Heuristik in virtueller Umgebung simuliert einen Computer im Computer, in dem Teile der Software auf gefährliches Verhalten überprüft wird. Diese proaktive Technologie stellt eine weitere Sicherheitsebene dar, die das Betriebssystem vor unbekannten Viren schützt, in dem gefährliche Kodierungen erkannt werden, für die noch keine Signaturen veröffentlicht wurden.

Permanenter Antivirenschutz. Die neuen und verbesserten BitDefender-Scan-Maschinen scannen und desinfizieren infizierte Dateien auf Befehl und minimieren den Datenverlust. Infizierte Dokumente können nun wiederhergestellt werden, anstatt wie früher gelöscht werden zu müssen.

Peer-2-Peer Applikationsschutz. Scannt nach Viren, die durch Instant Messaging und Filesharing-Software verteilt werden.

Kompletter E-Mail Schutz. Diese Anwendung funktioniert unter POP3 Protokollevel und bklockiert alle infizierten E-Mail Inhalte, ohne Rücksicht zu nehmen auf den genutzten E-Mail Client (MS Exchange, MS Outlook, MS Outlook Express, Netscape, Eudora, Lotus Notizs, Pegasus, The Bat, etc.) ohne zusätzliche Anwendungskonfiguration.

3.2. Erweiterte Funktionen

Stündliche Updates. Ohne dass der Nutzer eingreifen muss, werden neue, intelligente Updates zum Antivirenschutz heruntergeladen. Das Update kann über das Netzwerk, das Internet oder direkt über einen Proxy- Server ausgeführt werden. Ihr BitDefender Produkt ist sogar in der Lage, sich selbständig zu reparieren, indem beschädigte oder fehlende Dateien von unseren Servern heruntergeladen und neu installiert werden. Lizenzierte BitDefender-Nutzer profitieren somit von den kostenlosen Virendefinitionen, Updates und Produktverbesserungen.

Rund um die Uhr professioneller technischer Support. Qualifizierte Supportmitarbeiter geben Hilfestellung und online finden Sie eine Datenbank mit Antworten auf häufig gestellte Fragen (FAQ).

BitDefender Notfall CD. **BitDefender 9 Standard** wird mit einer bootfähigen CD (basierend auf LinuxDefender) ausgeliefert. Dies ermöglicht einen virenfreien Start des Systems über das CD ROM Laufwerk.

Kapitel 4. Die BitDefender Module

BitDefender 9 Standard beinhaltet die folgenden Module: **Allgemein**, **Antivirus** und **Update**.

4.1. Das Modul Allgemein

BitDefender verfügt über eine vollständige Konfiguration für maximale Sicherheit.

Wesentliche Status-Informationen über alle BitDefender-Module werden im Allgemein-Modul angezeigt. Hier können Sie das Produkt registrieren und Grundeinstellungen von BitDefender anpassen.

4.2. Das Modul Antivirus

BitDefender schützt alle gängigen Einstiegspunkte auf Ihrem System: E-Mail, Internet-Downloads, Instant Messaging, Netzwerkverbindungen und sämtliche Austauschdatenträger (CD, Diskette, ZIP, USB-Speicher). Vom Antivirus-Modul aus haben Sie Zugriff auf alle BitDefender-Einstellungen und BitDefender-Eigenschaften.

Der Virenschutz ist unterteilt in zwei Kategorien:

- Bei Zugriff scannen - verhindert, dass neue Viren Ihr System befallen. Dateien werden gescannt, sobald der Nutzer Zugriff darauf hat. BitDefender zum Beispiel scannt ein Worddokument auf Viren, sobald Sie es öffnen, und E-Mails, sobald Sie sie erhalten. BitDefender scannt Ihre Dateien, sobald Sie sie nutzen.
- Nach Aufforderung scannen - entdeckt residente Viren auf Ihrem System. Das ist der klassische Virenscan, ausgelöst durch den Nutzer – Sie wählen ein Laufwerk aus, einen Ordner oder eine Datei aus und BitDefender scannt sie – nach Aufforderung.

4.3. Das Modul Update

Da ständig neue Viren in relativ kurzen Abständen auftreten, ist es sehr wichtig, dass Sie Ihr Antiviren-Produkt täglich aktualisieren. BitDefender prüft in der Standard-Einstellung alle 1 Stunden auf verfügbare Updates.

Es gibt zwei Arten von Updates:

- **Antiviren-Schutz** - Täglich gibt es neue Bedrohungen für Ihren PC. Daher müssen die Virendefinitionen stets auf den neusten Stand gebracht werden. Diesen Vorgang nennt man **Virus Definitions Update**.

- **Produkt-Update** - Wenn eine neue Version von BitDefender erscheint, mit neuen Funktionen und Erkennungstechniken, die eine Verbesserung der Such- und Erkennungsleistung mit sich bringt. Diesen Vorgang nennt man **Product Update**.

Dem Anwender stehen zur Aktualisierung zwei Möglichkeiten zur Verfügung:

- **Automatisches Update** - BitDefender verbindet sich automatisch mit dem BitDefender- Update-Server und prüft, ob neue Updates vorhanden sind. Falls so angegeben, aktualisiert BitDefender sich automatisch.
- **Manuelles Update** - Der Benutzer entscheidet, wann BitDefender nach einem Update sucht.

Die Management Konsole

Kapitel 5. Überblick

BitDefender 9 Standard enthält eine zentrale Management-Konsole, die es erlaubt, die Schutzfunktionen für alle BitDefender-Module zu konfigurieren. Mit anderen Worten: Es reicht aus, die Management-Konsole zu öffnen, um Zugriff auf alle Module zu haben : **Antivirus** und **Update**.

Um die Management Konsole zu öffnen, klicken Sie im Startmenü auf **Programme** wählen Sie dort die Programmgruppe **BitDefender 9** und klicken Sie dort auf den Eintrag **BitDefender 9 Standard**. Sie können auch doppelt auf das **Symbol von BitDefender** in der System-Tray (neben der Uhr in der Taskleiste) klicken.

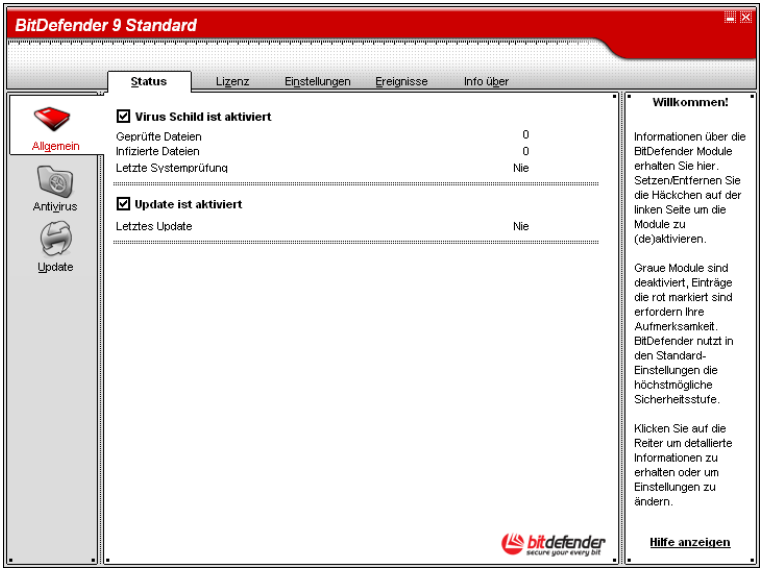

BitDefender 9 Standard
Status
Lizenz
Einstellungen
Ereignisse
Info über
Allgemein
Antivirus
Update
Virus Schild ist aktiviert
Geprüfte Dateien 0
Infizierte Dateien 0
Letzte Systemprüfung Nie
Update ist aktiviert
Letztes Update Nie
Willkommen!
Informationen über die BitDefender Module erhalten Sie hier. Setzen/Entfernen Sie die Häckchen auf der linken Seite um die Module zu (de)aktivieren.
Graue Module sind deaktiviert, Einträge die rot markiert sind erfordern Ihre Aufmerksamkeit. BitDefender nutzt in den Standard-Einstellungen die höchstmögliche Sicherheitsstufe.
Klicken Sie auf die Reiter um detaillierte Informationen zu erhalten oder um Einstellungen zu ändern.
Hilfe anzeigen

Abbildung 5.1. Management-Konsole

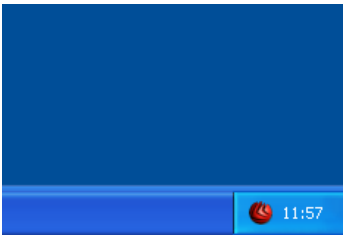
Auf der linken Seite der Management Konsole sehen Sie die Modul Auswahl:

- Allgemein - Sie sehen eine Zusammenfassung aller BitDefender-Einstellungen, überdies Produktdetails und Kontaktinformationen. Hier können Sie auch das Produkt registrieren.
- Antivirus - In diesem Bereich können Sie die **Antivirus** konfigurieren.
- Update - In diesem Bereich können Sie die **Update** konfigurieren.

Im rechten Bereich der Management Konsole sehen Sie stets Informationen zum jeweiligen Abschnitt, in dem Sie sich befinden. Die Option **Hilfe anzeigen**, platziert unten rechts, öffnet die **Hilfe**-Datei.

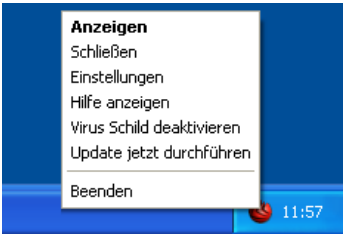
5.1. System Ablage

Wenn die Konsole minimiert ist, erscheint ein Symbol in der System Ablage:



Wenn Sie auf das Symbol doppelklicken, öffnet sich die Management-Konsole.

Abbildung 5.2. System Ablage



Mit einem Rechtsklick auf das Symbol, öffnet sich ein Pop Menü mit folgenden Optionen öffnet sich.

Abbildung 5.3. Kontextmenü

- **Anzeigen** - öffnet die Management Konsole.
- **Schließen** - minimiert das Programm.
- **Einstellungen** - öffnet den Abschnitt Einstellungen der Management Konsole.
- **Hilfe** - öffnet die Hilfe-Datei.

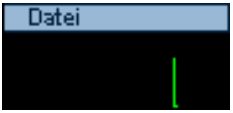
- **Virus Schild aktivieren / deaktiviert** - (de)aktiviert auf Wunsch den Echtzeitvirenschutz von BitDefender.
- **Jetzt aktualisieren** - führt unverzüglich ein Update von BitDefender durch, sofern verfügbar.
- **Beenden** - beendet die Anwendung. Bei Auswahl dieser Option, das Symbol in der Systemablage verschwindet und um erneut Zugriff auf die Management Konsole zu bekommen, starten Sie es aus dem Start Menü.

Anmerkung

- Wenn Sie ein oder mehrere Module von BitDefender deaktivieren verändert sich das Symbol von BitDefneder im System-Tray-Bereich. So werden Sie auch bei geschloßener Konsole über den Status von BitDefender informiert.
- Das BitDefender-Symbol blinkt wenn ein Update zur Verfügung steht.

5.2. Scan Aktionsbalken

Die **Scan Aktionsbalken** ist eine graphische Visualisierung der Prüfaktivität auf Ihrem System.



Die grünen Balken (die **Datei-Zone**) zeigen die Anzahl der gescannten Dateien pro Sekunde, auf einer Skala von 0 bis 50.

Abbildung 5.4. Scan Aktionsbalken

Anmerkung

Die **Scan activity bar** informiert Sie mit einem roten „X“, wenn das Virus Schild deaktiviert ist (**Datei**). Somit sind Sie über diesen Zustand auch informiert, wenn die Management Konsole nicht geöffnet ist.

Wenn Sie die graphische Visualisierung nicht länger sehen wollen, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Ausblenden**.

Anmerkung

Um das Fenster komplett zu verbergen, entfernen Sie das Häkchen bei **Aktivitätsanzeige einblenden** (im Abschnitt Einstellungen im Menüpunkt **Allgemein**).

Kapitel 6. Das Modul Allgemein

Der Abschnitt **Allgemein** behandelt und erklärt folgende Themen:

- Status aller BitDefender Module
- Registrierung des Produkts
- Allgemeine Einstellungen
- Ereignisanzeige
- Info über

Anmerkung

Weitere Inhalte und Einzelheiten zum Modul **Allgemein** finden Sie in der Produktbeschreibung auf Seite *„Das Modul Allgemein“* (S. 17).

6.1. Status aller BitDefender Module

Um diese Sektion zu öffnen klicken Sie bitte auf **Status** im Modul **Allgemein**.

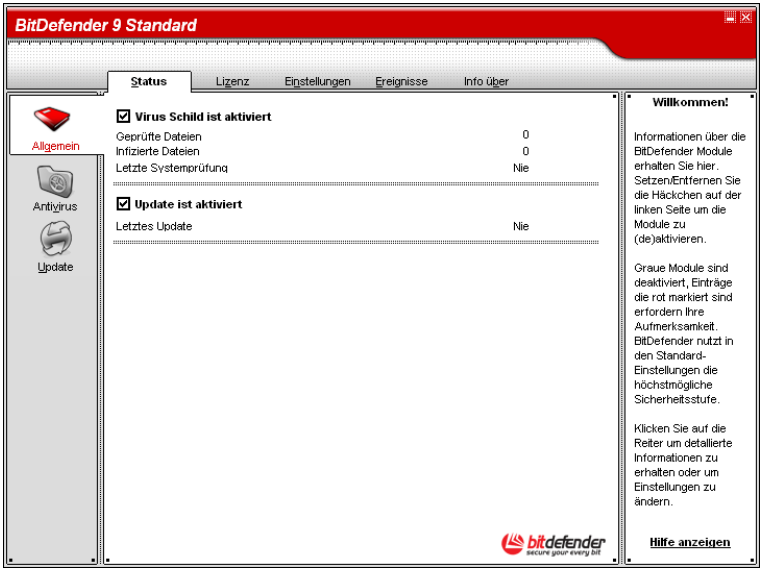

BitDefender 9 Standard
Status
Lizenz
Einstellungen
Ereignisse
Info über
Allgemein
Antivirus
Update
Virus Schild ist aktiviert
Geprüfte Dateien 0
Infizierte Dateien 0
Letzte Systemprüfung Nie
Update ist aktiviert
Letztes Update Nie
Willkommen!
Informationen über die BitDefender Module erhalten Sie hier. Setzen/Entfernen Sie die Häckchen auf der linken Seite um die Module zu (de)aktivieren.
Graue Module sind deaktiviert, Einträge die rot markiert sind erfordern Ihre Aufmerksamkeit. BitDefender nutzt in den Standard-Einstellungen die höchstmögliche Sicherheitsstufe.
Klicken Sie auf die Reiter um detallierte Informationen zu erhalten oder um Einstellungen zu ändern.
bitdefender
Hilfe anzeigen

Abbildung 6.1. Status

Hier finden Sie eine Übersicht über den Produkt-Status.

Durch Setzen der entsprechenden Häkchen können Sie die Hauptmerkmale des Bit-Defenders aktivieren oder deaktivieren.

Warnung

Optionen, die in Rot markiert sind, erfordern unbedingte Aufmerksamkeit

6.1.1. Virus Schild

Bietet einen Echtzeit-Schutz vor Viren und anderen gefährlichen Bedrohungen. Es zeigt die Anzahl der gescannten Dateien, der infizierten Dateien, der gescannten Nachrichten, der infizierten Nachrichten und das Datum des letzten System-Scans.

Anmerkung

Um zu verhindern, dass Viren Ihren Computer befallen, lassen Sie das **Virus Schild** immer aktiviert.

Warnung

Wir empfehlen dringend, einen kompletten Virenscan mindestens einmal in der Woche durchzuführen. Um einen kompletten Systemscan durchzuführen, aktivieren Sie das **Antiviren-Modul**, Sektion Prüfen, wählen Sie die **Lokalen Laufwerke** aus und klicken Sie dann auf **Prüfen**.

6.1.2. Automatisches Update

Neue Viren werden jeden Tag gefunden und identifiziert. Daher ist es sehr wichtig, BitDefender mit den neuesten Virensignaturen zu aktualisieren. Das Datum des letzten Updates und die Anzahl der Viren, die entdeckt (und somit auch desinfiziert) werden können, werden angezeigt.

Anmerkung

Damit Ihre wichtigen Daten stets geschützt sind, kann BitDefender ein automatisches Update durchführen. Lassen Sie daher am besten die Option **Automatisches update** aktiviert.

6.2. Registrierung des Produkts

Um diese Sektion zu öffnen klicken Sie bitte auf **Lizenz** im Modul **Allgemein**.

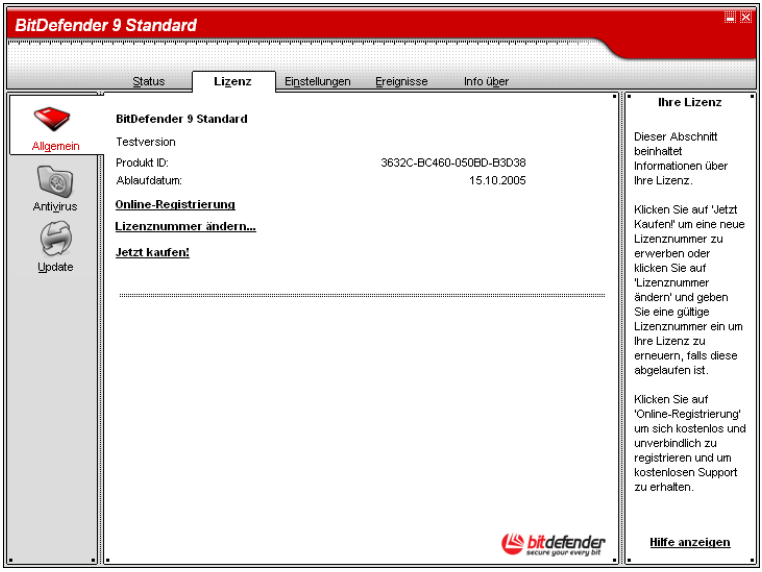


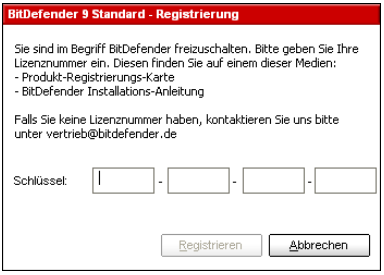
Abbildung 6.2. Registrierung des Produkts

Dieses Register zeigt Informationen über den Status Ihrer BitDefender-Lizenzen. Hier können Sie das Produkt registrieren und das Ablaufdatum sehen.

Das Produkt wird mit einem Test-Registrierungsschlüssel ausgeliefert, welcher eine Gültigkeit von 30 Tagen hat. Wenn Sie am Ende der Testzeit das Produkt erwerben wollen, benötigen Sie einen neuen Lizenzschlüssel. Klicken Sie hierfür auf **Jetzt kaufen**, um diesen im BitDefender- Online-Shop zu erhalten.

Zur Registrierung Ihres BitDefender Produktes klicken Sie bitte auf **Online Registrierung**, um sowohl den technischen Support als auch andere Serviceleistungen kostenlos nutzen zu können.

Um Ihren standardmäßigen Lizenzschlüssel zu erneuern, klicken Sie auf **Lizenznummer ändern**. Das folgende Fenster öffnet sich:


BitDefender 9 Standard - Registrierung
Sie sind im Begriff BitDefender freizuschalten. Bitte geben Sie Ihre Lizenznummer ein. Diesen finden Sie auf einem dieser Medien:
- Produkt-Registrierungs-Karte
- BitDefender Installations-Anleitung
Falls Sie keine Lizenznummer haben, kontaktieren Sie uns bitte unter vertrieb@bitdefender.de
Schlüssel:
Registrieren
Abbrechen

Tragen Sie Ihren **Schlüssel** in das entsprechende Feld ein. Klicken Sie auf **Registrieren**, um diesen Prozess abzuschließen.

Falls Sie sich verschreiben, werden Sie aufgefordert, Ihren Lizenzschlüssel erneut einzugeben.

Abbildung 6.3. Registrierung

Wenn Sie einen gültigen Lizenzschlüssel eingegeben haben, öffnet sich ein Bestätigungsfenster.

Nun können Sie in der Sektion **Registrierung** das Ablaufdatum Ihrer Lizenz einsehen.

6.3. Allgemeine Einstellungen

Um diese Sektion zu öffnen klicken Sie bitte auf **Einstellungen** im Modul **Allgemein**.

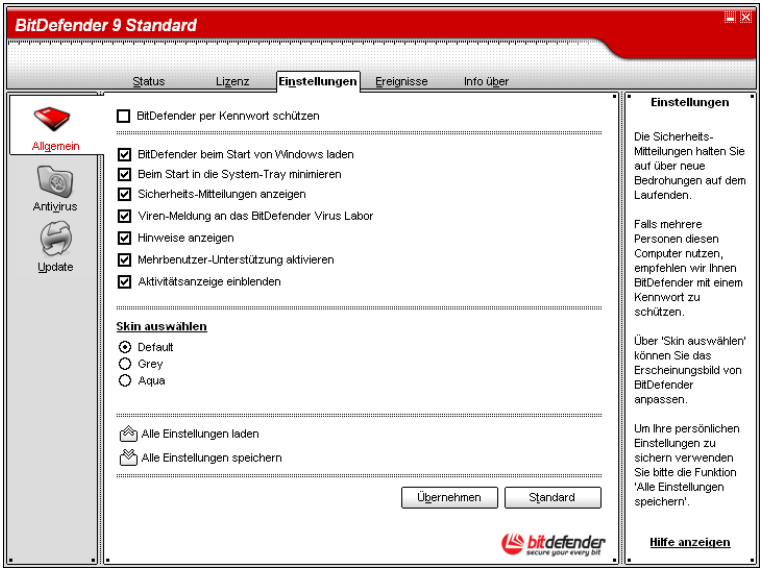


Abbildung 6.4. Allgemeine Einstellungen

Hier können Sie die umfassenden Einstellungen von BitDefender einsehen. Standardmäßig wird BitDefender beim Windowsstart geladen und läuft dann im Hintergrund.

Die folgenden Optionen sind verfügbar:

- **Konsole per Kennwort schützen** - die Passwort-Einstellung aktivieren, um Ihre BitDefender-Einstellungen zu schützen;

  Anmerkung

  Wenn Sie nicht der einzige Benutzer des Computers sind, empfehlen wir Ihnen, Ihre vorgenommenen Einstellungen mit einem Passwort zu schützen.

  Das folgende Fenster erscheint:

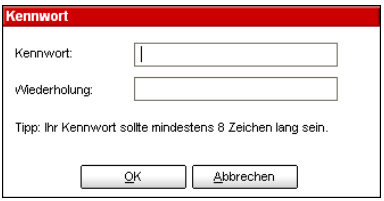


Abbildung 6.5. Kennwort bestätigen

Schreiben Sie ein Passwort in das **Kennwort**-Feld und wiederholen Sie es in das **Kennwort erneut**-Feld. Danach klicken Sie auf **OK**.

Von nun an werden Sie stets aufgefordert, Ihr Passwort einzugeben, wenn Sie die Einstellungen von BitDefender ändern wollen.

Wichtig

Falls Sie Ihr Passwort vergessen haben sollten, müssen Sie unter Reparieren Ihre BitDefender-Konfiguration modifizieren.

- **BitDefender beim Start von Windows laden** - automatisches Starten des BitDefenders beim Systemstart.

Anmerkung

Dies wird dringend empfohlen.

- **Minimiert starten** - minimiert die BitDefender-Management-Konsole, nachdem das System gestartet worden ist. Nur das BitDefender Symbol erscheint in der Systemablage.
- **Sicherheits-Mitteilungen anzeigen** - von Zeit zu Zeit empfangen Sie Sicherheitsmeldungen, die von BitDefender-Servern versendet werden.
- **Startbildschim anzeigen** - zeigt das Fenster, welches geöffnet wird, wenn Sie BitDefender starten.
- **Viren-Meldung an das BitDefender Virus Labor** - sendet erkannte Viren an das BitDefender-Virenlabor. Diese Meldung zeigt uns die Verbreitung von Viren an und hilft uns, geeignete Gegenmaßnahmen ergreifen zu können.

  Der Report enthält keinerlei vertrauliche Daten, wie z. B. Ihren Namen oder Ihre IP-Adresse, und wird nicht für kommerzielle Zwecke verwendet. Die gelieferten Informationen enthalten den Virennamen und werden lediglich für statistische Zwecke benötigt.

- **Hinweise anzeigen** - Pop-up-Fenster anzeigen, die über den Produktstatus informieren.
- **Mehrbenutzer-Unterstützung aktivieren** - erlaubt anderen Benutzern die Verwendung von BitDefender mit persönlichen Einstellungen.

Anmerkung

Diese Option kann nur von Benutzern mit Administrator-Rechten verändert werden.

- **Aktivitätsanzeige aktivieren** - Zum Aktivieren bzw. Deaktivieren die Abschnitt 5.2, *„ Scan Aktionsbalken “* [23].
- **Oberflächen** - Datei erlaubt Ihnen, die Farbe der Management-Konsole zu wählen. Der Skin repräsentiert die Hintergrundgrafiken und Symbolfarben in der Benutzeroberfläche. Klicken Sie auf die jeweilige Bezeichnung, um die Benutzeroberfläche gemäß Ihren Wünschen anzupassen.

Verwenden Sie die Option **Alle Einstellungen speichern** / **Alle Einstellungen laden** um eine Sicherungskopie sämtlicher in BitDefender vorgenommenen Einstellungen zu exportieren und nach einer Reparatur wieder zu importieren.

Klicken Sie auf **Übernehmen** um die Einstellungen zu speichern. Wenn Sie auf **Standard** klicken werden die Werkseinstellungen geladen.

6.4. Ereignisanzeige

Um diese Sektion zu öffnen, klicken Sie bitte auf **Ereignisse** im Modul **Allgemein**.

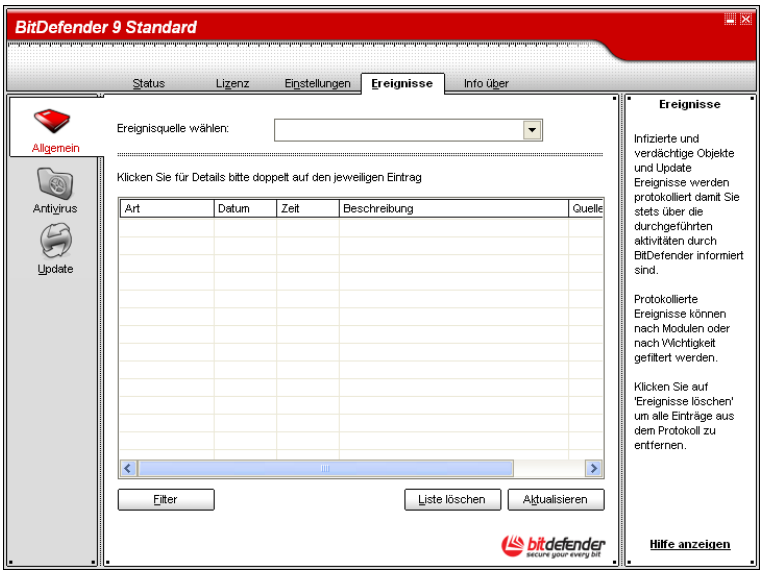


Abbildung 6.6. Ereignisse

In dieser Sektion sind sämtliche von BitDefender erstellten Ereignisse angezeigt.

Es gibt drei Arten von Ereignissen: **Information**, **Warnung** und **Kritisch**.

Beispiel für solche Ereignisse:

- **Information** - Wenn eine E-Mail überprüft wurde;
- **Warnung** - Wenn eine verdächtige Datei gefunden wurde;
- **Kritisch** - Wenn eine infizierte Datei gefunden wurde.

Für jedes Ereignis werden die folgenden Informationen bereitgestellt: Datum und Uhrzeit, zu der das jeweilige Ereignis stattgefunden hat, eine kurze Beschreibung und seine Quelle (**Antivirus** oder **Update**). Klicken Sie doppelt auf ein bestimmtes Ereignis und Sie erhalten weitere Informationen zu diesem Thema.

Es ist möglich, die angezeigten Ereignisse auf zwei Arten zu filtern – nach Quelle oder nach Art:

- Klicken Sie auf **Filter** und wählen Sie die gewünschte Ereignisart aus;

- Wählen Sie die **Ereignisquelle**, aus der gleichnamigen Dropdownliste;

Ist die Sektion **Ereignisse** bereits geöffnet, so müssen Sie auf die Schaltfläche **Aktualisieren** klicken, um neu hinzu gekommene Ereignisse anzeigen zu lassen.

Um alle Ereignisse zu löschen, klicken Sie bitte auf die Schaltfläche **Liste löschen**.

6.5. Info über

Um diese Sektion zu öffnen klicken Sie bitte auf **Info über** im Modul **Allgemein**.

BitDefender 9 Standard
Status
Lizenz
Einstellungen
Ereignisse
Info über
Allgemein
Antivirus
Update
BitDefender 9 Professional Plus
Build 9.0
Kontaktinformationen:
Copyright (c) 2001-2005 SOFTWIN GmbH. Alle Rechte vorbehalten.
Web-Seiten
http://www.softwin.de/
http://www.bitdefender.de/
E-Mail-Adressen
vertrieb@bitdefender.de
support@bitdefender.de
Telefon
0 75 42 - 94 44 44
Telefax
0 75 42 - 94 44 99
Bitte lesen Sie die FAQs bevor Sie den Technischen Support kontaktieren:
http://www.bitdefender.de/bd/site/animiert.php
http://www.bitdefender.de/bd/site/support.php?menu_id=15
Über BitDefender
BitDefender® bietet Sicherheitslösungen für die täglichen Sicherheits-anforderungen von Computern und zum Schutz vor Bedrohungen bei mehr als 41 Millionen Privat- und Firmenkunden in mehr als 100 Ländern.
BitDefender® ist von den unabhängigen Instituten ICSA Labs, CheckMark, Virus Bulletin und dem TÜV Saarland zertifiziert. Des Weiteren ist BitDefender die einzige Sicherheits-lösung welche mit dem 'IST Price' ausgezeichnet wurde.
Hilfe anzeigen

Abbildung 6.7. Allgemeine Informationen

In dieser Sektion finden Sie Kontaktinformationen und Produktdetails.

BitDefender bietet Sicherheitslösungen an, die den heutigen Computerumgebungen gerecht werden, und liefert effektives Gefahrenmanagement für über 41 Millionen Heimanwender und Unternehmen in mehr als 100 Länder.

BitDefender ist zertifiziert von allen größeren unabhängigen Kritikern - **ICSA Labs**, **CheckMark** und **Virus Bulletin** und überdies das einzige Sicherheitsprodukt, das einen **Preis von IST** erhalten hat.

Kapitel 7. Das Modul Antivirus

Der Abschnitt **Antivirus** behandelt und erklärt folgende Themen:

- Bei Zugriff scannen
- Nach Aufforderung prüfen
- Prüfen mit BitDefender-Planer
- Quarantäne
- Berichte

Anmerkung

Weitere Inhalte und Einzelheiten zum Modul **Antivirus** finden Sie in der Produktbeschreibung auf Seite *„Das Modul Antivirus“* (S. 17).

7.1. Bei Zugriff scannen

Um diese Sektion zu öffnen klicken Sie bitte auf **Schild** im Modul **Antivirus**.

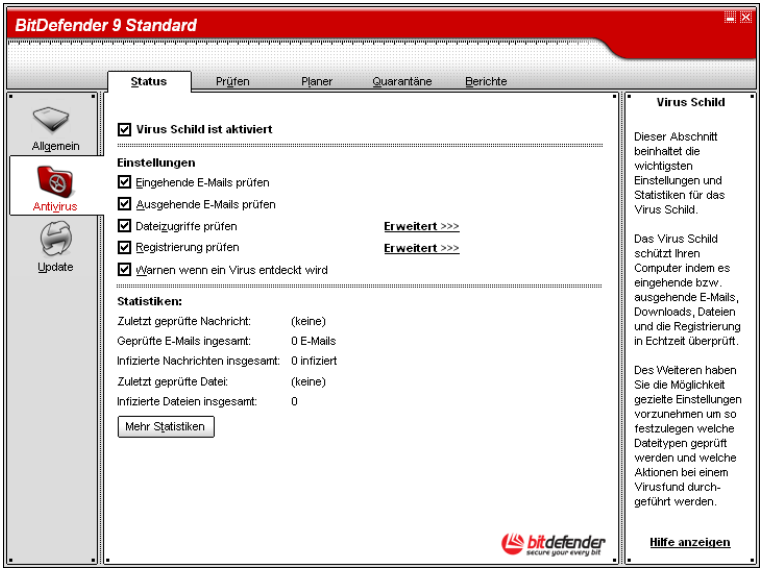

BitDefender 9 Standard
Status
Prüfen
Planer
Quarantäne
Berichte
Allgemein
Antivirus
Update
Virus Schild ist aktiviert
Einstellungen
Eingehende E-Mails prüfen
Ausgehende E-Mails prüfen
Dateizugriffe prüfen
Erweitert >>>
Registrierung prüfen
Erweitert >>>
Warnen wenn ein Virus entdeckt wird
Statistiken:
Zuletzt geprüfte Nachricht: (keine)
Geprüfte E-Mails insgesamt: 0 E-Mails
Infizierte Nachrichten insgesamt: 0 infiziert
Zuletzt geprüfte Datei: (keine)
Infizierte Dateien insgesamt: 0
Mehr Statistiken
Virus Schild
Dieser Abschnitt beinhaltet die wichtigsten Einstellungen und Statistiken für das Virus Schild.
Das Virus Schild schützt Ihren Computer indem es eingehende bzw. ausgehende E-Mails, Downloads, Dateien und die Registrierung in Echtzeit überprüft.
Des Weiteren haben Sie die Möglichkeit gezielte Einstellungen vorzunehmen um so festzulegen welche Dateitypen geprüft werden und welche Aktionen bei einem Virusfund durchgeführt werden.
Hilfe anzeigen

Abbildung 7.1. Virus Schild

In diesem Abschnitt können Sie das **Virus Schild** konfigurieren und Informationen über dessen Aktivität einsehen. Das **Virus Schild** schützt alle gängigen Einstiegspunkte auf Ihrem System: E-Mail, Internet- Downloads, Instant Messaging, Netzwerkverbindungen und sämtliche Austauschdatenträger (CD, Diskette, ZIP, USB-Speicher).

Anmerkung

Um zu verhindern, dass Viren Ihren Computer befallen, aktivieren Sie das **Virus Schild**.

Am unteren Ende dieser Registerkarte sehen Sie die **Virus Schild** -Statistik über Dateien und E-Mail-Nachrichten. Klicken Sie auf **Mehr Statistiken**, wenn Sie mehr Informationen erhalten wollen.

7.1.1. Wichtigsten Einstellungen

Um eine Auswahl zu treffen, klicken Sie auf die entsprechende Box.

- **Eingehende E-Mails prüfen** - prüft alle eingehende E-Mail-Nachrichten.
- **Ausgehende E-Mails prüfen** - prüft alle ausgehenden E-Mail-Nachrichten.
- **Dateizugriffe prüfen** - alle Dateien werden von BitDefender überprüft.
- **Warnen wenn ein Virus entdeckt wurde** - zeigt eine Warnmeldung an wenn ein Virus in einer Datei oder E-Mail gefunden wurde.

  Bei infizierten Datei wird eine Warnmeldung ausgegeben die Hinweise über die Art des Schädlings beinhaltet. Bei infizierten E-Mails erhält der Empfänger eine Nachricht mit Hinweisen über die Art des Schädlings und Informationen über den Absender der Nachricht.

  Im Falle eines Verdachts kann ein Assistent aufgerufen werden der Ihnen dabei hilft verdächtige Dateien zur weiteren Analyse an das BitDefender Virus Labor zu senden. Optional können Sie Ihre E-Mail-Adresse angeben um weitere Informationen zur Analyse zu erhalten.

7.1.2. Anderer Optionen

Fortgeschrittene Benutzer können über die erweiterten Einstellungen BitDefender nach Ihren Wünschen anpassen. So können bestimmte Dateierweiterungen oder Archive vom Prüfvorgang ausgenommen werden. Klicken Sie hierzu auf **Erweitert** >>> analog zur **Dateizugriffe prüfen**.

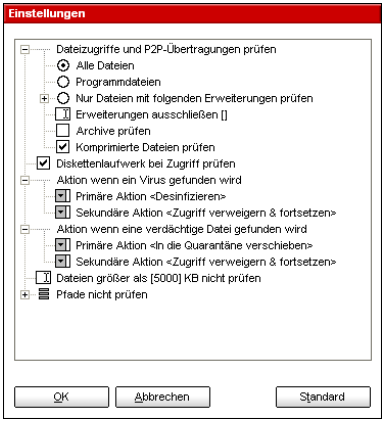


Abbildung 7.2. Schild Einstellungen

Klicken Sie auf "+", um eine Option zu öffnen, und auf "-", um diese zu schließen.

Sie können sehen, dass einige Prüf-optionen sich nicht öffnen lassen, obwohl das "+"- Zeichen sichtbar ist. Der Grund dafür ist, dass diese Optionen bisher nicht gewählt worden sind. Wenn Sie diese Optionen auswählen, können sie geöffnet werden.

- **Dateizugriffe und P2P-Übertragungen prüfen** - um alle Dateien und die Kommunikation mit Instant Messengers (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger) zu überprüfen. Des Weiteren wählen Sie eine Datei aus, die Sie prüfen möchten.

  Die folgenden Optionen sind wählbar:

Optionen	Beschreibung
Alle Dateien prüfen	Prüft alle vorhanden Dateien.
Programmdateien	Prüft ausschließlich Dateien mit den Dateiendungen: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html;

Optionen	Beschreibung
	.xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml und .nws.
Nur Dateien mit folgenden Erweiterungen	Nur die Dateien werden überprüft, die der Nutzer spezifiziert hat. Weitere Dateien müssen mit ";" getrennt werden.
Erweiterungen ausschließen	Nur die Dateien werden NICHT geprüft, die der Nutzer spezifiziert hat. Weitere Dateien müssen mit ";" getrennt werden.
Archive prüfen	Auch der Inhalt von Archiven wird geprüft. Ist diese Option aktiviert, so kann es zur Verlangsamung des Computers führen.
Komprimierte Dateien prüfen	Alle komprimierten Dateien werden überprüft.
Prüfen auf Riskware (Gefahrengut)	Prüft auf Gefahren wie Dialer, Spyware und Adware. Entsprechende Riskware - Dateien werden wie infizierte Dateien behandelt. Software mit Adware-Komponenten arbeitet unter Umständen nicht mehr, wenn diese Option aktiviert ist.

- **Diskettenlaufwerk bei Zugriff prüfen** - wenn Sie das Laufwerk prüfen wollen.
- **Primäre Aktion** - wählen Sie aus der Liste die erste Aktion für infizierte Dateien. BitDefender erlaubt im Falle eines Virenfundes zwei Aktionen.

  Folgende Optionen sind wählbar:

Aktion	Beschreibung
Zugriff verhindern und fortfahren	Im Falle eines Virenfundes wird der Zugriff auf die Datei verhindert.
Datei säubern	Um die infizierte Datei zu desinfizieren.
Datei löschen	Die infizierte Datei wird ohne Warnung sofort gelöscht.

Aktion	Beschreibung
In Quarantäne verschieben	Die infizierte Datei wird in die Quarantäne verschoben.

- **Sekundäre Aktion, falls primäre fehlschlägt** - Wählen Sie hier eine Aktion, die ausgeführt werden soll, wenn die primäre Aktion fehlschlägt.

  Folgende Optionen sind wählbar:

Aktion	Beschreibung
Zugriff verhindern und fortfahren	Im Falle eines Virenfundes wird der Zugriff auf die Datei verhindert.
Datei löschen	Die infizierte Datei wird ohne Warnung sofort gelöscht.
In Quarantäne verschieben	Die infizierte Datei wird in die Quarantäne verschoben.

  Für verdächtig erscheinende Dateien besteht dieselbe Einstellungsmöglichkeit wie für infizierte Dateien.

- **Dateien größer als [x] nicht prüfen** - geben Sie die maximale Größe der zu prüfenden Datei ein. Falls die Größe 0 Kb ist, werden alle Dateien geprüft.
- **Pfade nicht prüfen** - Klicken Sie auf " + " um einen Ordner auszuwählen, der nicht geprüft werden soll. Die Konsequenz ist, dass die Option ausgeweitet wird und `Neues Objekt` erscheint. Klicken Sie auf die dazu gehörende Box und wählen Sie aus dem Fenster die Datei aus, die nicht geprüft werden soll.

Klicken Sie auf **OK** um die Einstellungen zu speichern. Wenn Sie auf **Standard** klicken werden die Werkseinstellungen geladen.

7.2. Nach Aufforderung prüfen

Um diese Sektion zu öffnen klicken Sie bitte auf **Prüfen** im Modul **Antivirus**.

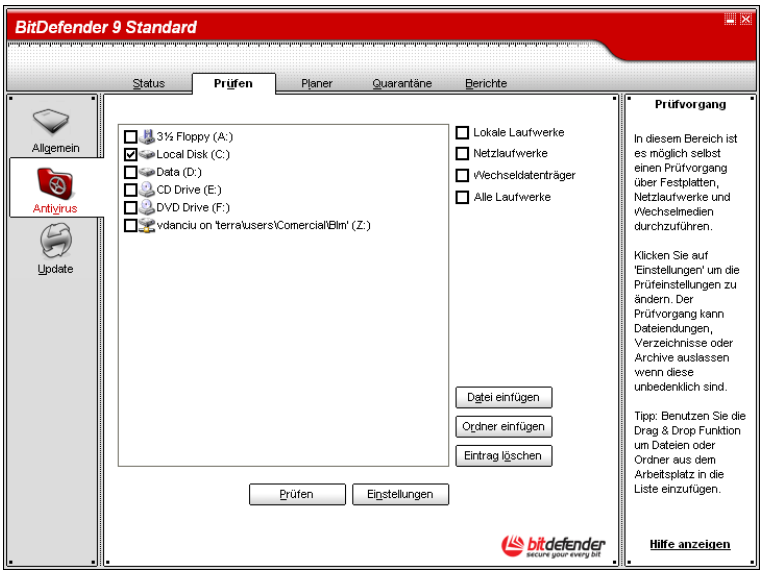


Abbildung 7.3. Prüfen

In diesem Fenster können Sie die BitDefender Einstellungen zur Prüfung Ihres Computers vornehmen.

Die Mission der BitDefender-Software ist es sicherzustellen, dass es keine Viren in Ihrem System gibt. Dies wird in erster Linie erreicht, indem Ihre E-Mail-Anhänge und Downloads überprüft und alle Aktionen, die auf Ihrem System stattfinden, überwacht werden.

Es besteht aber die Gefahr, dass ein Virus bereits in Ihrem System ist, bevor Sie BitDefender installieren. Deshalb es ist eine sehr gute Idee, Ihren Computer auf residente Viren zu prüfen, nachdem Sie BitDefender installiert haben. Übrigens es ist auch eine gute Idee, Ihren Computer häufig auf Viren zu prüfen.

BitDefender ermöglicht vier Arten, auf Anforderung zu prüfen:

- Sofortiges prüfen - folgen Sie den unten angegebenen Schritten, um Ihren Computer auf Viren zu prüfen;

- Kontextbezogenes Prüfen - Rechtsklick auf eine Datei oder einen Ordner und wählen Sie im Kontextmenü BitDefender Antivirus v9 aus;
- Prüfen per Drag & Drop - verschieben Sie mittels Drag & Drop eine Datei oder einen Ordner auf die Aktivitätsleiste;
- Prüfen mit BitDefender-Planer - die Systemüberprüfung wird periodisch oder zu bestimmten Zeitpunkten ausgeführt.

7.2.1. Sofortiges prüfen

Um "auf Anforderung" zu prüfen, muss wie folgt vorgegangen werden:

Schritt 1/5 - Schließen Sie alle offenen Anwendungen

Damit Sie einen vollständigen Suchlauf mit BitDefender durchführen können, ist es wichtig, alle Programme zu beenden. Besonders wichtig ist, dass Sie Ihr E-Mail Programm schließen (z. B. Outlook, Outlook Express oder Eudora).

Schritt 2/5 - Stellen Sie sicher, dass BitDefender auf dem aktuellen Stand ist

Da es täglich neue Bedrohungen durch Viren und Würmer gibt, sollten Sie, bevor Sie den Suchlauf starten, BitDefender mit Hilfe des Update Moduls aktualisieren.

Schritt 3/5 - Öffnen Sie die Antivirus Sektion

In der Management Konsole klicken Sie auf **Antivirus** und Prüfen. Anfänglich enthält diese Sektion ein Abbild der Partitionsstruktur Ihres Systems. Außerdem sind einige Schaltflächen und Prüfoptionen sichtbar.

Dieser Bereich enthält folgende Schaltflächen:

- **Datei hinzufügen** - diese Schaltfläche ermöglicht das Hinzufügen bestimmter, zu prüfender Dateien. Wenn Sie hierauf klicken, können Sie die Dateien im nächsten sich öffnenden Fenster auswählen.

- **Ordner hinzufügen** - diese Schaltfläche ermöglicht das Hinzufügen eines neuen, zu prüfenden Ordners. Wenn Sie hierauf klicken, können Sie den Ordner im nächsten sich öffnenden Fenster auswählen.

Anmerkung

Ziehen Sie per Drag & Drop Dateien und Ordner auf die Prüfen-Sektion, um diese der Liste der zu prüfenden Objekte zuzufügen.

- **Eintrag löschen** - löscht die Datei/denOrdner, die/der vorher ausgewählt wurde.

Anmerkung

Nur die Dateien/Ordner, die nachträglich hinzugefügt wurden, können gelöscht werden. Dateien/Ordner, die von BitDefender vorgegeben wurden, können nicht gelöscht werden.

- **Einstellungen** - ermöglicht die Auswahl der zu prüfenden Dateien, die gewünschte Aktion, falls eine infizierte Datei gefunden wird, die Art der Berichterstattung sowie die Erstellung einer Berichtsdatei mit den Prüfungsergebnissen.
- **Prüfen** - startet den Prüfvorgang des Systems mit den ausgewählten Prüfoptionen.

Optionen, die das schnelle Auswählen der Scan-Ziele erlauben.

- **Lokale Laufwerke** - prüft die lokalen Laufwerke.
- **Netzlaufwerke** - prüft die verfügbaren Netzwerklaufwerke.
- **Wechseldatenträger** - prüft alle entfernbaren Laufwerke (CD-ROM-Laufwerke, Diskettenlaufwerke).
- **Alle Laufwerke** - prüft alle Laufwerke: lokale, entfernbare oder verfügbare Netzwerklaufwerke.

Anmerkung

Zur schnellen Auswahl aller Laufwerke klicken Sie auf **Alle Laufwerke** auswählen.

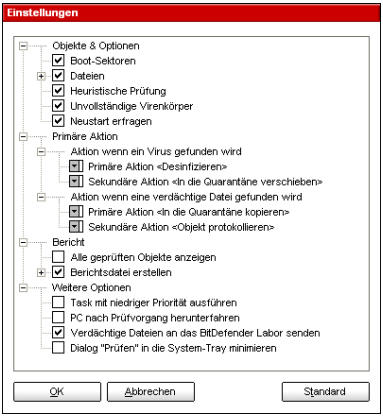
Wichtig

Klicken Sie dann einfach auf den **Prüfen**-Button. BitDefender prüft ihren Computer nun unter Verwendung der Standard-Einstellungen.

Schritt 4/5 - Auswählen der Prüfoptionen

Benutzer mit Vorkenntnissen sollten sich die Prüfeinstellungen von BitDefender genauer ansehen. Bestimmte Dateierweiterungen, Verzeichnisse und Archive, die wahrscheinlich keine Bedrohung darstellen, können vom Scan ausgeschlossen werden. So wird die Prüfzeit verringert und das Reaktionsvermögen Ihres Rechners während eines Scans verbessert.

Klicken Sie auf **Einstellungen** von Prüfen , um mehr zu erfahren.



Die Prüfeinstellungen sind wie ein aufklappbares Windows-Explorermenü aufgebaut.

Abbildung 7.4. Einstellungen

Die Prüf-Optionen sind in vier Kategorien unterteilt:

- **Prüfoptionen**
- **Aktionsoptionen**
- **Berichtoptionen**
- **Performance-Optionen**

Anmerkung

Um eine Option zu öffnen bzw. zu schließen, klicken Sie auf das Kästchen mit dem "+"- bzw. dem "-"-Zeichen.

- Geben Sie an, welche Arten von Objekte geprüft werden sollen (Archiv, Postfächer, etc.). Weitere Optionen können über die Kategorie **Prüfoptionen** angegeben werden.

Die folgenden Optionen zur Erkennung sind verfügbar:

Einstellungen		Beschreibung
Boot-Sektoren		Prüft die Bootsektoren des Systems.
Dateien	**Alle**	Prüft alle vorhandenen Dateien, benötigt die meiste Zeit und findet auch versteckte oder getarnte Viren.
	Programmdateien	Prüft ausschließlich Dateien mit den Dateiendungen: exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml und nws.
	Nur Dateien mit folgenden Erweiterungen	Prüft nur Dateien mit benutzerdefinierten Erweiterungen. Sie bestimmen, welche Daten geprüft werden sollen (Einschlussprinzip). Weitere Dateien müssen mit ";" getrennt werden.
	Folgende Erweiterungen ausschließen	Prüft alle Dateien, außer denen mit benutzerdefinierten Erweiterungen. Sie bestimmen, welche Daten nicht geprüft werden sollen (Ausschlussprinzip). Weitere Dateien müssen mit ";" getrennt werden.
	Komprimierte Dateien	Alle komprimierten Dateien werden überprüft.
	Archive	Prüft den Inhalt von eingepackten Archiven.
	Postfächer	Prüft den Inhalt von E-Mails und deren Attachments.
Heuristische Prüfung		Aktiviert den heuristischen Suchmodus. Mittels Heuristik können bisher unbekannte Viren auf Grundlage bestimmter Aktionsmuster und Verhaltensweisen, entdeckt werden. Dabei kann es auch zu Fehlalarmen kommen. Sollte eine verdächtige Datei auf Ihrem System

Einstellungen	Beschreibung
	gefunden werden, empfehlen wir, die Datei zur Überprüfung an das BitDefender-Virus-Labor zu schicken.
Unvollständige Virenkörper	Spürt unvollständige Virenkörper auf.
Prüfen auf Riskware (Gefahren-gut)	Prüft auf Gefahren wie Dialer, Spyware und Adware. Entsprechende Riskware - Dateien werden wie infizierte Dateien behandelt. Software mit Adware-Komponenten arbeitet unter Umständen nicht mehr, wenn diese Option aktiviert ist.
Neustart erfragen	Falls eine Aktion den Neustart des Computers erfordert, dies signalisieren und den Neustart beim Benutzer erfragen.

- Wählen Sie die Aktionen für infizierte und verdächtige Dateien aus. Öffnen Sie die **Aktionsoptionen**, um alle möglichen Aktionen für diese Dateien anzeigen zu lassen.

  Wählen Sie die Aktion, die durchzuführen ist, wenn eine infizierte oder verdächtige Datei gefunden wird. Sie können unterschiedliche Vorgehensweisen für infizierte und verdächtige Dateien festlegen. Sie können außerdem eine sekundäre Aktion festlegen, wenn die Primäre fehlschlägt.

Aktion	Beschreibung
Objekte protokollieren	Es wird keine Aktion für infizierte Dateien ausgeführt. Diese Dateien finden Sie Berichtsdatei.
Benutzer abfragen	Bei einer entdeckten Infektion muss der Benutzer die weiteren Aktionen bestätigen. Folgende Optionen stehen zur Verfügung: Desinfizieren, in der Quarantäne Isolieren oder Löschen.
Dateien reparieren	Reinigt die infizierte Datei von dem schädlichen Programmcode.

Aktion	Beschreibung
Dateien löschen	Löscht automatisch, ohne Warnung, alle infizierten Dateien.
Dateien umbenennen	Die Infizierte Datei wird umbenannt. Die neue Erweiterung der infizierten Dateien wird `.vir` sein. Durch die Umbenennung von infizierten Dateien ist es nicht länger möglich diese Dateien auszuführen, um somit eine weitere Verbreitung zu verhindern. Außerdem kann die Datei für weitere Analysezwecke gespeichert werden.
In die Quarantäne kopieren	Kopiert infizierte Dateien in die Quarantäne. Dies bedeutet, dass eine infizierte Datei in die Quarantäne kopiert wird. Die Originaldatei bleibt weiterhin infiziert im Originalverzeichnis bestehen. Es kann weiterhin auf Sie zugegriffen werden und der schädliche Code ausgeführt werden.
In die Quarantäne verschieben	Verschiebt die infizierte Datei in die Quarantäne.

- Optionen für Berichtsdateien angeben. Öffnen Sie die **Berichtsoptionen** um alle möglichen Optionen anzeigen zu lassen.

Optionen		Beschreibung
Alle geprüften Objekte anzeigen		Zeigt in einer Berichtdatei den Status und mögliche Infektionen aller geprüften Dateien an. Ist diese Option aktiviert, so kann es zur Verlangsamung des Computers führen.
Berichtdatei erstellen	**Berichtdatei**`vscan.log`	In diesem Feld können Sie den Namen der Berichtdatei festlegen. Klicken Sie auf die Beschreibung und geben Sie den neuen Dateinamen ein.
	Zum vorhandenen Bericht hinzufügen	Wählen sie diese Option aus, wenn Sie die Informationen über den neuen Prüfvorgang zu einer schon vorhandenen Berichtdatei hinzufügen möchten.

Optionen	Beschreibung
Berichtdatei auf [1024] KB begrenzen	Im Laufe der Zeit können sich große Berichtdateien entwickeln. Klicken Sie, um die Größe der Berichtdatei zu begrenzen, auf das Kästchen und geben Sie in das angezeigte Feld die maximale Größe der Datei in KB ein.

Anmerkung

Die Berichtsdatei kann im Abschnitt Berichte im Menüpunkt **Antivirus** eingesehen werden.

- Festlegen weiterer Optionen. Öffnen Sie den Abschnitt **Erweitert**, um folgende Optinen auszuwählen:

Aktion	Beschreibung
Aufgaben mit niedriger Priorität ausführen	Herabstufung der Priorität des Prüfvorgangs. Andere Programme werden somit schneller ausgeführt. Der gesamte Prüfvorgang dauert damit aber entsprechend länger.
Herunterfahren des Computers nach erfolgtem Prüfvorgang	Der Rechner wird nach erfolgtem Prüfvorgang ausgeschaltet.
Versenden verdächtiger Dateien an das BitDefender Labor	Sie haben die Möglichkeit, verdächtige Dateien zur Prüfung an das BitDefender Labor zu schicken.
Minimieren des Prüffensters beim Scan-Start	Es verkleinert das Prüffenster beim Prüfvorgang in die untere Symbolleiste. Es kann durch einen Doppelklick auf das BitDefender – Logo in der Symbolleiste wieder geöffnet werden.

Klicken Sie auf **OK** um die Einstellungen zu speichern. Wenn Sie auf **Standard** klicken werden die Werkseinstellungen geladen.

Schritt 5/5 - Prüfung starten

Nachdem Sie die Prüfoptionen bestimmt haben, müssen Sie nur noch den Prüfvorgang starten, indem Sie auf **Prüfen** klicken. Dieser Vorgang kann, abhängig von der Größe Ihrer Festplatte, einen Moment dauern.

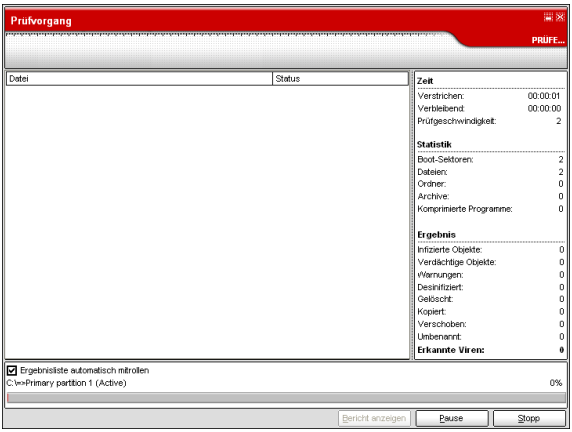


Abbildung 7.5. Prüfvorgang

Während eines Prüfvorgangs zeigt BitDefender den Forschritt dessen und Warnungen über gefundene Schädlinge an.

Wählen Sie die Checkbox **Zuletzt geprüfte Dateien anzeigen** und Sie sehen nur Informationen über die zuletzt geprüften Dateien.

Drei Schaltflächen sind verfügbar:

- **Stop** - Ein neues Fenster öffnet sich und Sie werden gefragt, ob Sie die Systemprüfung stoppen möchten. Klicken Sie auf **Ja&Schließen**, um das Fenster für den Prüfvorgang zu schließen.
- **Pause** - Hält den Prüfvorgang für eine bestimmte Zeit an; klicken Sie auf **Fortsetzen**, um ihn wieder zu starten.
- **Bericht anzeigen** - Der Prüfbericht wird geöffnet und die zurzeit überprüften Dateien werden laufend angezeigt.

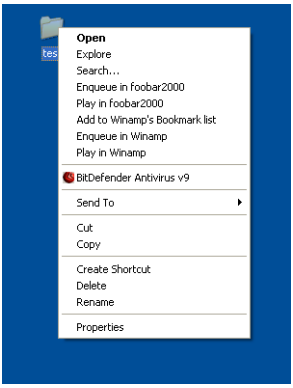
Anmerkung

Die Berichtsdatei wird automatisch im Abschnitt Berichte im Menüpunkt **Antivirus** gesichert.

Es wird ein Symbol in der System-Tray angezeigt, wenn ein Prüfvorgang aktiv ist.

7.2.2. Scannen mit dem Kontextmenü

Klicken Sie mit der rechten Maustaste auf die zu prüfende Datei. Wählen Sie **BitDefender Antivirus v9** aus.



Es wird eine Berichtsdatei namens `vscan.log` erstellt. Diese kann über den Abschnitt Berichte im Menüpunkt **Antivirus** angezeigt werden.

Abbildung 7.6. Kontextmenü

7.2.3. Prüfen per Drag & Drop

Ziehen Sie die gewünschte Datei auf den **Datei-/Netzprüfmonitor**, wie auf den folgenden Bildern dargestellt.

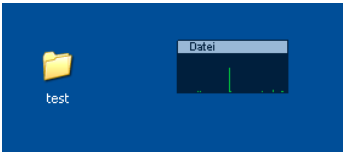


Abbildung 7.7. Herüberziehen der Datei

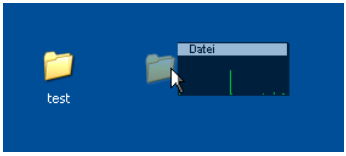
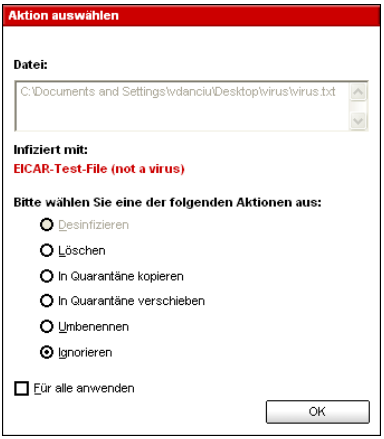


Abbildung 7.8. Ablegen der Datei

Es wird eine Berichtsdatei namens `activbar.log` erstellt. Diese kann über den Abschnitt Berichte im Menüpunkt **Antivirus** angezeigt werden.

In einem neuen Fenster werden der Vorgang und das Ergebnis der Prüfung angezeigt. Wird ein Schädling entdeckt, so erhalten Sie ein Alarm-Fenster angezeigt und werden aufgefordert, eine Aktion auszuwählen.



Hier sehen Sie den Namen der Datei und des Virus.

Abbildung 7.9. Auswahl für Aktionen

Nun können Sie eine der folgenden Möglichkeiten auswählen:

- **Desinfizieren** - reinigt die infizierten Dateien;
- **Löschen** - löscht automatisch alle infizierten Dateien, ohne eine Warnmeldung auszugeben;
- **In die Quarantäne kopieren** - kopiert infizierte Dateien in die Quarantäne;
- **In die Quarantäne verschieben** - verschiebt die infizierten Dateien in die Quarantäne;
- **Umbenennen** - benennt die infizierten Dateien um. Die neue Erweiterung der infizierten Dateien `.vir` sein.
- **Ignorieren** - In diesem Fall wird die Infizierung ignoriert und keine Aktion ausgeführt.

Wenn Sie einen gesamten Ordner überprüfen und die ausgewählte Aktion auf alle gefundenen Schädlinge übertragen möchten, so wählen Sie bitte die Option **Für alle anwenden**.

Anmerkung

Ist die Option **Desinfizieren** nicht verfügbar, so bedeutet dies, das die Datei nicht desinfiziert werden kann. Die beste Alternative ist, die Datei in der Quarantäne zu isolieren und diese später zwecks Analyse an das Virenlabor zu senden.

Klicken Sie auf **OK**.

7.2.4. Prüfen mit dem BitDefender Planer

Um diese Sektion zu öffnen klicken Sie bitte auf **Planer** im Modul **Antivirus**.

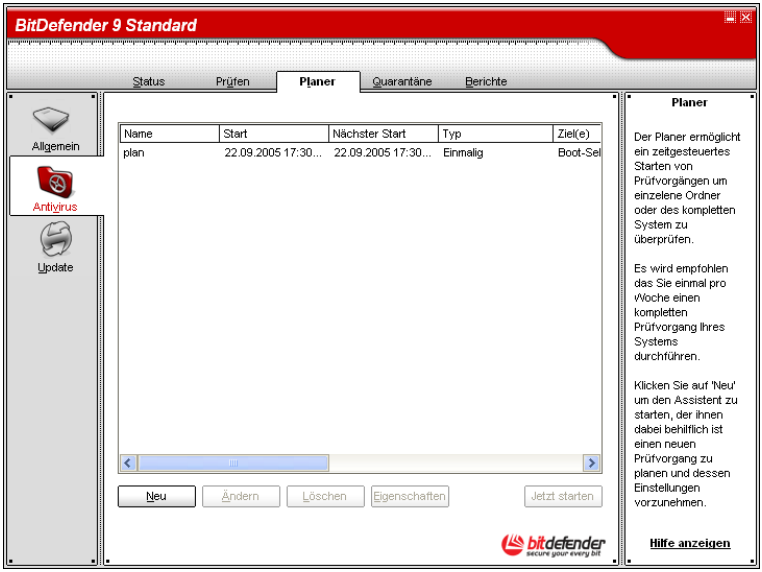


Abbildung 7.10. Antivirus Planer

Durch den BitDefender-Planer wird die Systemüberprüfung periodisch oder zu bestimmten Zeitpunkten ausgeführt, ohne dass der Benutzer eingreifen muss. Dazu wird vorher ein so genannter Task, eine Aufgabe oder ein Ereignis erstellt.

Der **Planer** enthält einen Assistenten, mit dem neue Aufgaben erstellt werden. Er wird Ihnen jedes Mal Hilfe leisten, wenn Sie ein neues Ereignis erstellen möchten oder ein schon vorhandenes ändern möchten.

Hier finden Sie einige Schaltflächen, die zur Verwaltung der Prüfaufgaben dienen.

- **Neu** - startet den Assistenten, der Sie bei der Erstellung eines neuen Prüf-Ereignisses unterstützt.
- **Ändern** - ändert die Eigenschaften eines vorher erstellten Ereignisses. Dabei wird ebenfalls der Assistent gestartet.

Anmerkung

Falls sich der Ereignisname ändert, wird ein neues Ereignis erstellt.

- **Löschen** - löscht ein ausgewähltes Ereignis.
- **Jetzt starten** - startet sofort die ausgewählte Aufgabe.
- **Eigenschaften** - zeigt die Eigenschaften eines ausgewählten Ereignisses an.

Die Benutzeroberfläche des Planers enthält ebenfalls eine Liste, in der die Prüfereignisse angezeigt werden. Diese enthalten den Namen des Prüfereignisses, das Datum der ersten Ausführung, das Datum der nächsten Ausführung und die Prüfart (periodisch oder einmalig).

Wenn Sie einen geplanten Prüfvorgang mit der rechten Maustaste anklicken, erscheint ein Kontextmenü, welches dem oben beschriebenen ähnelt.

Anmerkung

Der **Planer** erlaubt eine nicht limitierte Anzahl von geplanten Vorgängen.

Sie können auch mit der Tastatur durch die Scan-Ereignisse surfen: drücken Sie die **Löschtaste**, um das gewählte Scan-Ereignis zu löschen, drücken Sie die **Eingabetaste**, um die gewählten Ereigniseigenschaften anzusehen oder die **Inserttaste** , um ein neues Ereignis zu erstellen (der Planer-Assistent erscheint).

Anmerkung

Drücken Sie die Pfeiltasten, um in der Ereignisliste zu navigieren.

Klicken Sie auf **Neu**, um einen neuen geplanten Vorgang zu erstellen. Dies öffnet den Assistenten, der Sie Schritt für Schritt bei der Erstellung eines Zeitplans unterstützt.

Schritt 1/9 - Willkommensfenster

Abbildung 7.11. Willkommen

Geben Sie den Namen des neuen Ereignisses in das Feld **Name** ein und fügen Sie eine kurze Beschreibung in das Feld **Beschreibung** ein.

Die folgenden Optionen sind wählbar:

- **Aufgaben mit niedriger Priorität ausführen** - Herabstufung der Priorität des Prüfvorgangs. Andere Programme werden somit schneller ausgeführt. Der gesamte Prüfvorgang dauert damit aber entsprechend länger.
- **Minimieren des Prüffensters beim Scan-Start** - Es verkleinert das Prüffenster beim Prüfvorgang in die untere Symbolleiste. Es kann durch einen Doppelklick auf das BitDefender – Logo in der Symbolleiste wieder geöffnet werden.
- **Herunterfahren des Computers nach erfolgtem Prüfvorgang** - Der Rechner wird nach erfolgtem Prüfvorgang ausgeschaltet.

Klicken Sie auf **Weiter**, um fortzufahren. Wenn Sie **Abbrechen** anklicken, öffnet sich ein Fenster, in dem Sie Ihre Entscheidung bestätigen: die Task-Erstellung abzubrechen oder fortzusetzen.

Schritt 2/9 - Start datum und zeit

Abbildung 7.12. Start datum und zeit

Wählen Sie die Häufigkeit der durchzuführenden Prüfungen:

- **Einmalig** - startet den Prüfvorgang zu einem festgelegten Zeitpunkt einmalig.
- **Regelmäßig** - startet den Prüfvorgang in festgelegten Zeitabständen (Stunden, Tage, Wochen, Monate, Jahre) beginnend mit einem fest definierten Zeitpunkt (Datum & Uhrzeit).

Falls die Prüfung nach einer bestimmten Zeitspanne wiederholt werden soll, klicken Sie auf **Periodisch** und danach geben Sie in das **Eingabe-Kästchen** die Anzahl der Minuten / Stunden / Tage / Wochen / Jahre ein und der Prozess wird nach dem Ablauf der angegebenen Zeitspanne wiederholt.

Anmerkung

Sie können auf die Pfeile klicken, um die Minuten-/Stunden-/Tage-/Wochen-/Jahres-zähler höher oder niedriger einzustellen.

Sie können auf die Pfeile klicken, um die Minuten-/Stunden-/Tage-/Wochen-/Jahres-zähler höher oder niedriger einzustellen.

Wichtig

Falls Sie die Option für ein wiederholtes Prüfen ausgewählt haben, ist der Prüfvorgang zeitlich unbegrenzt. Um dieses Ereignis zu verwerfen, muss es von der Ereignisliste aus dem Planerfenster gelöscht werden.

Auf Wunsch schliesst sich das Prüffenster automatisch, falls keine verdächtigen oder infizierten Dateien gefunden wurden. Dazu markieren Sie bitte diese Option mit einem Häkchen.

Klicken Sie auf **Zurück**, um zum vorherigen Fenster zu gelangen, oder klicken Sie auf **Weiter**, um fortzufahren .

Schritt 3/9 - Zielobjekte

Abbildung 7.13. Zielobjekte

Sie können eines der folgenden Objekte auswählen:

- **Boot-Sektoren** - prüft den Bootsektor, um Bootviren zu erkennen;
- **Dateien** - prüft den Arbeitsspeicher des Systems, um im Arbeitsspeicher vorhandene Viren zu entdecken;
- **Postfachdateien** - prüft Mailarchive, um Mailviren zu entdecken;
- **Archive** - prüft Archivinhalte;
- **Komprimierte Dateien** - prüft komprimierte Dateien.

Wählen Sie eines oder mehrere Zielobjekte aus, indem Sie diese(s) einfach anklicken.

Klicken Sie auf **Zurück**, um zum vorherigen Fenster zu gelangen, oder klicken Sie auf **Weiter**, um fortzufahren .

Schritt 4/9 - Zielpfad

Abbildung 7.14. Zielpfad

Weiterhin müssen Sie den Pfad des zu prüfenden Objektes auswählen. Dieser Schritt ist notwendig, falls Sie im dritten Schritt die **Prüfung von Dateien** ausgewählt haben.

Nebenstehend wird das Explorerfenster angezeigt, aus dem Sie die zu prüfenden Partitionen, Ordner und Dateien auswählen können. Wenn sich der Mauszeiger auf einer Datei befindet, wird der vollständige Pfad der Datei in dem Feld unter dem Explorer-fenster angezeigt.

Anmerkung

Klicken Sie auf das Kästchen mit dem "+"-Zeichen, um einen Pfad zu öffnen oder auf das "-" –Zeichen, um einen Pfad zu schließen.

Um die zu prüfenden Adressen auszuwählen, können Sie auch die Schnellauswahl verwenden, die sich über dem Explorerfenster befindet:

- **Lokale Laufwerke** - prüft alle lokalen Laufwerke;
- **Netzlaufwerke** - prüft alle Netzwerklaufwerke.

Klicken Sie auf **Zurück**, um zum vorherigen Fenster zu gelangen, oder klicken Sie auf **Weiter**, um fortzufahren .

Schritt 5/9 - Dateimaske

Abbildung 7.15. Dateimaske

Weiterhin müssen Sie die Art der zu prüfenden Dateien auswählen. Dieser Schritt ist notwendig, falls Sie im dritten Schritt die **Prüfung von Dateien** ausgewählt haben.

Nebenstehend wird das Explorerfenster angezeigt, aus dem Sie die zu prüfenden Partitionen, Ordner und Dateien auswählen können. Wenn sich der Mauszeiger auf einer Datei befindet, wird der vollständige Pfad der Datei in dem Feld unter dem Explorer-fenster angezeigt.

Sie müssen sich für eine einzige Kategorie entscheiden:

- **Alle** - prüft alle Dateitypen;
- **Ausführbare & Dokumente** - prüft Programmdateien und Dokumente;
- **Aus dieser Liste** - prüft nur die Dateien, deren Erweiterungen nicht in der Liste erscheinen.

Anmerkung

Diese Erweiterungen müssen durch ein Semikolon getrennt werden.

Falls Sie Informationen zu allen geprüften, infizierten oder nicht infizierten Dateien sehen möchten, wählen Sie die Option **Alle geprüften Dateien anzeigen**. Aber bedenken Sie, dass sich Ihre Computerleistung mit dieser Einstellung reduziert.

Klicken Sie auf **Zurück**, um zum vorherigen Fenster zu gelangen, oder klicken Sie auf **Weiter**, um fortzufahren .

Schritt 6/9 - Analyse Typ

Abbildung 7.16. Analyse Typ

Weiterhin müssen Sie die Prüfart auswählen:

- **Keine Heuristik verwenden** - bedeutet, dass die Dateien anhand von Virensignaturen geprüft werden;
- **Heuristik verwenden** - stellt eine auf bestimmten Algorithmen basierende Methode dar. Sie dient dem Zweck neue, noch unbekannte Viren zu entdecken. Gelegentlich können dadurch vermeintlich verdächtige Codes in normalen Programmen gemeldet werden (Fehlalarm).

Die folgenden Optionen sind wählbar:

- **Versenden verdächtiger Dateien an das BitDefender Labor** - Sie haben die Möglichkeit, verdächtige Dateien zur Prüfung an das BitDefender Labor zu schicken.
- **Prüfen auf Riskware (Gefahrengut)** - Prüft auf Gefahren wie Dialer, Spyware und Adware. Entsprechende Riskware - Dateien werden wie infizierte Dateien behandelt. Software mit Adware-Komponenten arbeitet unter Umständen nicht mehr, wenn diese Option aktiviert ist.

Klicken Sie auf **Zurück**, um zum vorherigen Fenster zu gelangen, oder klicken Sie auf **Weiter**, um fortzufahren .

Schritt 7/9 - Aktionsoptionen

Abbildung 7.17. Aktionsoptionen

Wählen Sie dann zwei Aktionen aus, die im Fall eines Virenfundes ausgeführt werden sollen. Wählen Sie die Aktionen für infizierte und verdächtige Dateien aus.

Aktion	Beschreibung
Objekte protokollieren	Es wird keine Aktion für infizierte Dateien ausgeführt. Diese Dateien finden Sie Berichtsdatei.
Benutzer abfragen	Bei einer entdeckten Infektion muss der Benutzer die weiteren Aktionen bestätigen. Folgende Optionen stehen zur Verfügung: Desinfizieren, in der Quarantäne isolieren oder Löschen.
Dateien reparieren	Reinigt die infizierte Datei von dem schädlichen Programmcode.
Dateien löschen	Löscht automatisch, ohne Warnung, alle infizierten Dateien.
Dateien umbenennen	Ändert die Extension der infizierten Datei. Die neue Extension ist `.vir`. Durch die Umbenennung der infizierten Datei werden die Infektion des Systems und die weitere Verbreitung des Virus verhindert. Und die Datei steht für weitere Prüfung und Analyse zur Verfügung.
In die Quarantäne copieren	Kopiert infizierte Dateien in die Quarantäne. Dies bedeutet, dass eine infizierte Datei in die Quarantäne kopiert wird. Die Originaldatei bleibt weiterhin infiziert im Originalverzeichnis bestehen. Es kann weiterhin auf Sie zugegriffen werden und der schädliche Code ausgeführt werden.

Aktion	Beschreibung
In die Quarantäne verschieben	Verschiebt die infizierte Datei in die Quarantäne. Somit kann auf die Datei nicht mehr zugegriffen werden.

Anmerkung

Wir empfehlen Ihnen, **Desinfizieren** als erste und **In die Quarantäne verschieben** als zweite Aktion auszuwählen.

Für verdächtig erscheinende Dateien besteht dieselbe Einstellungsmöglichkeit wie für infizierte Dateien.

Klicken Sie auf **Zurück**, um zum vorherigen Fenster zu gelangen, oder klicken Sie auf **Weiter**, um fortzufahren .

Schritt 8/9 - Bericht

Abbildung 7.18. Bericht

Um einen Bericht zu erstellen, klicken Sie auf **Bericht erstellen**. Damit werden auch alle anderen Optionen für die Berichterstellung aktiviert.

Geben Sie den Namen des Berichts in das Feld **Dateiname** ein. Standardname ist `schedule.log`. Der Bericht beinhaltet Informationen über den Scanprozess: die Anzahl der entdeckten Viren, die Anzahl der geprüften Dateien, die Anzahl der desinfizierten und entfernten Viren.

Sie können die maximale Dateigröße der Berichtsdatei einschränken, indem Sie den entsprechenden Wert in das dazugehörige Eingabefeld eintragen.

Anmerkung

Die Berichtsdatei kann im Abschnitt Berichte im Menüpunkt **Antivirus** eingesehen werden.

Klicken Sie auf **Zurück**, um zum vorherigen Fenster zu gelangen, oder klicken Sie auf **Weiter**, um fortzufahren .

Schritt 9/9 - Zusammenfassung

Abbildung 7.19. Zusammenfassung

Dies ist der letzte Schritt des Assistenten. In diesem Fenster können Sie sämtliche Einstellungen zur Kontrolle einsehen. Änderungen können vorgenommen werden, indem Sie auf **Zurück** klicken und die jeweiligen Optionen ändern.

Falls Sie keine weiteren Änderungen vornehmen möchten, klicken Sie auf **Fertigstellen**.

Das neue Ereignis wird nun im Planerfenster angezeigt.

7.3. Quarantäne

Um diese Sektion zu öffnen klicken Sie bitte auf **Quarantäne** im Modul **Antivirus**.

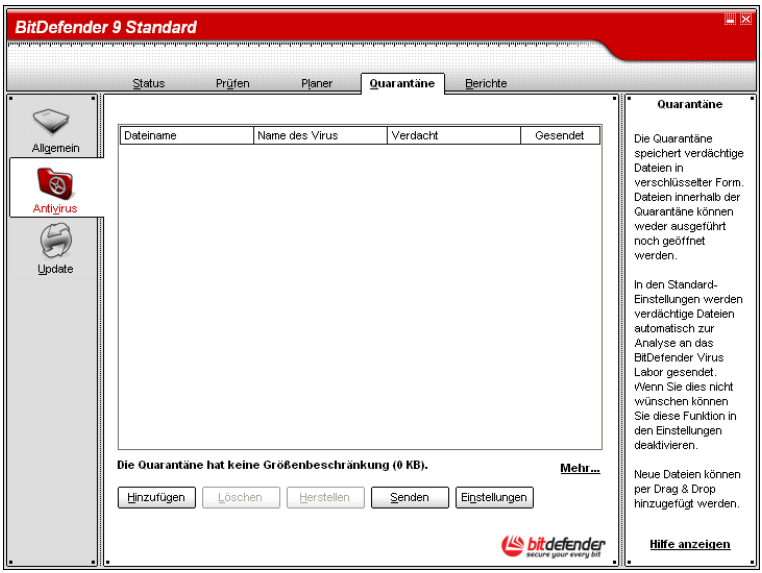


Abbildung 7.20. Quarantäne

BitDefender ermöglicht die Isolation von infizierten Dateien in einem sicheren Bereich, der so genannten Quarantäne. Durch die Isolation der infizierten Dateien in der Quarantäne reduziert sich das Risiko einer weiteren Infektion. Die infizierten Dateien können zur genaueren Analyse automatisch oder manuell an das BitDefender-Labor gesendet werden.

Der Bestandteil, der die Verwaltung der isolierten Dateien sicherstellt, ist die **Quarantäne**. Dieses Modul enthält eine Funktion, die die infizierten Dateien auf Wunsch automatisch zum BitDefender-Labor sendet.

Wenn eine Prüfung ausgeführt wird, kann der Benutzer die Optionen so konfigurieren, dass eine Berichtdatei erstellt und Informationen über den Prüfvorgang angezeigt werden. Diese Informationen kann der Benutzer direkt in der Management-Konsole betrachten.

Wie Sie sicherlich bereits festgestellt haben, enthält der Abschnitt **Quarantäne** eine Liste aller Dateien, die isoliert wurden. Zu jeder Datei sind die folgenden Informationen

verfügbar: Name, Dateigröße, Isolationsdatum, und Übertragungsdatum. Um weitere Informationen anzuzeigen, klicken Sie bitte auf **Mehr Infos**.

Anmerkung

Die in der Quarantäne enthaltenen Dateien können weder ausgeführt noch geöffnet werden.

Die **Quarantäne** -Oberfläche enthält folgende Buttons.

- **Hinzufügen** - Fügt Dateien zur Quarantäne hinzu. Falls Sie wissen oder glauben, dass Sie eine infizierte Datei auf Ihrem Rechner haben, können Sie diese im Quarantäneordner isolieren. Ein neues Fenster öffnet sich und Sie können die Datei auswählen. Damit wird die Datei in die Quarantäne copieren.

  Wenn Sie die Datei in die Quarantäne-Zone verschieben möchten, wählen Sie die Checkbox **Original-Datei(en) löschen** aus. Eine weitere Methode, infizierte Dateien in die Quarantäne zu verschieben, ist, sie per drag&drop in das Quarantäne-Feld zu ziehen.

- **Löschen** - entfernt die ausgewählte Datei;

- **Wiederherstellen** - stellt markierte Dateien im Ursprungsverzeichnis wieder her.

- **Senden** - Sie können diese Dateien zur gründlichen Analyse an das BitDefender-Labor senden.

  Wichtig

  Sie müssen zunächst weitere Informationen angeben, bevor Sie Dateien übertragen. Klicken Sie zunächst auf **Einstellungen** und füllen Sie dort das Feld **E-Mail-Adresse** aus.

- **Einstellungen** - Öffnet die erweiterten Optionen für den Abschnitt Quarantäne. Das folgende Fenster öffnet sich:

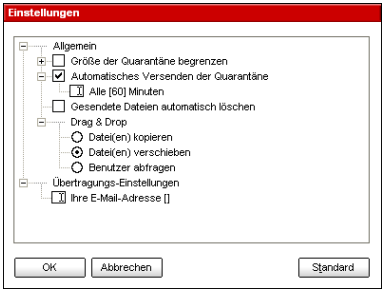


Abbildung 7.21. Einstellungen

Die Quarantäne-Einstellungen sind in zwei Kategorien unterteilt:

- **Allgemein**
- **Übertragungs-Einstellungen**

Anmerkung

Klicken Sie auf das Kästchen mit dem "+"-Zeichen, um eine Option zu öffnen, oder auf das "-"-Zeichen, um eine Option zu schließen.

Allgemein

- **Größe der Quarantäne begrenzen** - Hält die Größe der Quarantäne unter Kontrolle. Diese Option ist in der Voreinstellung aktiviert und liegt bei 12.000 KB. Wenn Sie diesen Wert ändern möchten, klicken Sie bitte in das Eingabefeld und tragen Sie einen neuen Wert ein.
- **Automatisches Versenden der Quarantäne** - sendet automatisch alle Dateien aus dem Quarantäne-Ordner zur Überprüfung an das BitDefender-Virenlabor. Sie können das Intervall bestimmen, in dem der Inhalt der Quarantäne automatisch versendet wird.
- **Gesendete Dateien automatisch löschen** - löscht automatisch die aus der Quarantäne gesendeten Dateien.
- **Drag&Drop** - für die Drag & Drop-Funktion des Quarantäne-Ordners können Sie hier die Art des Drag & Drop einstellen: Kopieren der Dateien, Verschieben der Dateien, Benutzer abfragen.

Übertragungs-Einstellungen

- **Ihre E-Mail-Adresse** - geben Sie hier Ihre E-Mail-Adresse an, wenn Sie eine Antwort bezüglich der eingesendeten Dateien aus dem Virenlabor haben möchten.

7.4. Berichte

Um diese Sektion zu öffnen klicken Sie bitte auf **Berichte** im Modul **Antivirus**.

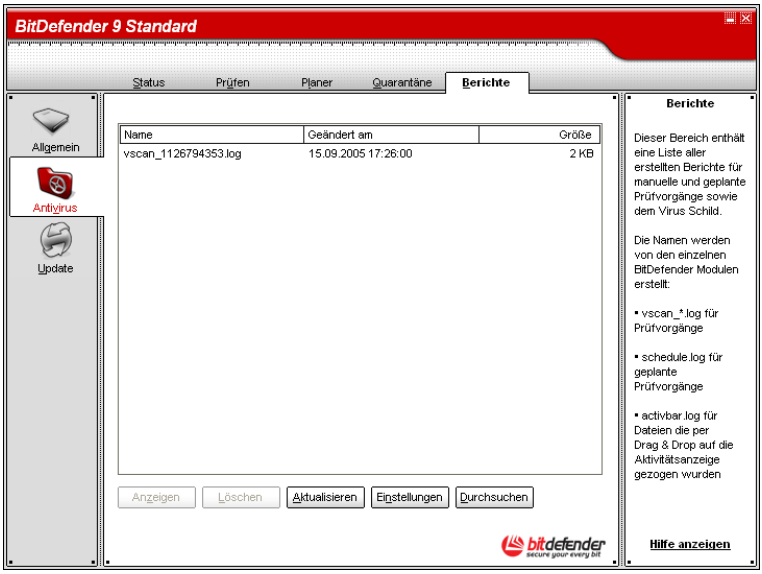


Abbildung 7.22.

Der **Berichtbereich** enthält eine Liste aller Berichtdateien die bisher generiert wurden. Bei jeder Datei werden Name, Größe und Datum der letzten Änderung angezeigt.

Wenn eine Prüfung ausgeführt wird, kann der Benutzer die Optionen so konfigurieren, dass eine Berichtdatei erstellt und Informationen über den Prüfvorgang angezeigt werden. Diese Informationen kann der Benutzer direkt in der Management-Konsole betrachten.

BitDefender zeichnet alle seine Aktivitäten und Ergebnisse auf Ihrem Computer auf. Folgende Statistiken stehen Ihnen zur Verfügung:

- Vscan.log diese Datei wird geschrieben, wenn Sie eine manuelle Systemprüfung starten;
- Schedule.log enthält die Ergebnisse der geplanten Suchläufe, die Sie festgelegt haben;
- Activbar.log wird erstellt, wenn Sie mit Drag & Drop möglicherweise infizierte Dateien prüfen.

Der Abschnitt **Berichte** beinhaltet mehrere Schaltflächen zur Verwaltung der einzelnen Berichte. Die Funktion der jeweiligen Schaltfläche erklärt sich wie folgt:

- **Anzeigen** - öffnet die ausgewählte Berichtdatei;
- **Löschen** - löscht die ausgewählte Berichtdatei;
- **Aktualisieren** - Aktualisiert den Abschnitt **Berichte**. Falls in der Management-Konsole das Register **Berichte** geöffnet ist und in der Zwischenzeit ein Prüfvorgang auf Ihrem Computer stattfindet, wird die neue Berichtdatei mit den Prüfergebnissen (wenn Sie die Option Dateibericht erstellen ausgewählt haben) nur dann angezeigt, wenn sie auf **Aktualisieren** klicken.
- **Durchsuchen** - öffnet ein Fenster, in welchem Sie die Berichtdateien, die Sie sich ansehen wollen, auswählen können.

Anmerkung

Die Berichtdateien (die im Berichtbereich erscheinen) werden im selben Ordner gespeichert, in dem BitDefender installiert wurde. Wenn Sie die Berichtdateien in einem anderen Ordner gespeichert haben, klicken Sie auf **Durchsuchen**, um diese Dateien zu finden.

Kapitel 8. Das Modul Update

Der Abschnitt **Update** behandelt und erklärt folgende Themen:

- Automatisches Update
- Manuelles Update
- Update-Einstellungen

Anmerkung

Weitere Inhalte und Einzelheiten zum Modul **Update** finden Sie in der Produktbeschreibung auf Seite *„Das Modul Update“* (S. 18).

8.1. Das automatische Update

Um diese Sektion zum öffnen, klicken Sie bitte **Status** im Modul **Update**.

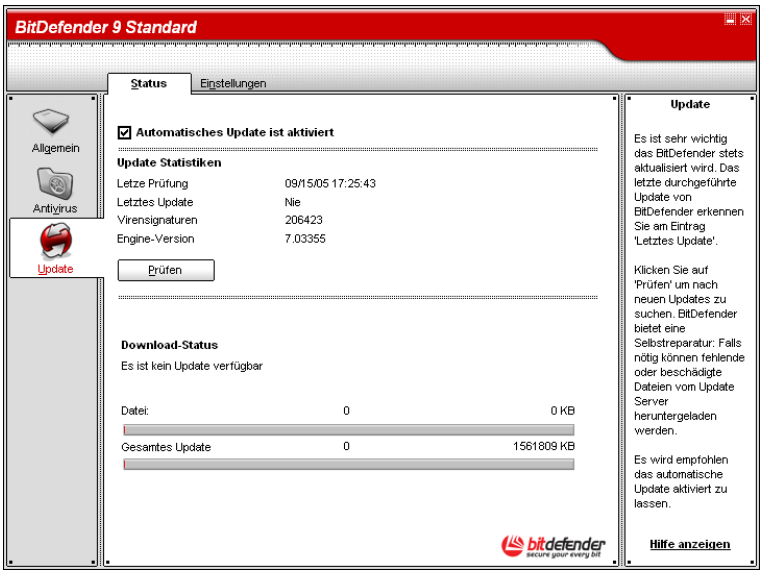

BitDefender 9 Standard
Status
Einstellungen
Allgemein
Antivirus
Update
Automatisches Update ist aktiviert
Update Statistiken
Letze Prüfung 09/15/05 17:25:43
Letztes Update Nie
Virensignaturen 206423
Engine-Version 7.03355
Prüfen
Download-Status
Es ist kein Update verfügbar
Datei: 0 0 KB
Gesamtes Update 0 1561809 KB
Update
Es ist sehr wichtig das BitDefender stets aktualisiert wird. Das letzte durchgeführte Update von BitDefender erkennen Sie am Eintrag 'Letztes Update'.
Klicken Sie auf 'Prüfen' um nach neuen Updates zu suchen. BitDefender bietet eine Selbstreparatur: Falls nötig können fehlende oder beschädigte Dateien vom Update Server heruntergeladen werden.
Es wird empfohlen das automatische Update aktiviert zu lassen.
Hilfe anzeigen

Abbildung 8.1. Status

Falls Sie über eine Breitbandverbindung, oder eine DSL-Verbindung verfügen, arbeitet BitDefender eigenständig. Es prüft beim Start des Computers, ob neue Virensignaturen verfügbar sind und fährt nach Bedarf sogar **stündliche** Updates.

Wenn ein neues Update verfügbar ist, handelt BitDefender je nach vorgenommener Einstellung im Menü Einstellungen. Entweder werden Sie darum gebeten, den neu verfügbaren Download jetzt herunter zu laden, oder das Update erfolgt automatisch.

Anmerkung

Sie können die vorgenommenen Einstellungen des automatischen Updates in dem Menü *„Update-Einstellungen“* (S. 76) jederzeit ändern.

Das automatische Update kann auch jederzeit über den Klick **Prüfen** erfolgen. Diese Funktion wird auch als **benutzergesteuertes Update** bezeichnet.

Das **Update** Modul verbindet Ihren Computer mit dem BitDefender Update Server und benachrichtigt Sie bei einem neu verfügbaren Update. Wenn ein neues Update

verfügbar ist, wird je nach vorgenommener Einstellung entweder darum gebeten, das Update Download jetzt herunter zu laden, oder das Update erfolgt automatisch.

Wichtig

Möglicherweise kann ein Neustart nach dem vollständig durchgeführten Update notwendig werden. Wir empfehlen Ihnen, den Neustart möglichst bald durchzuführen.

Anmerkung

Falls Sie über eine Internet by Call Verbindung verfügen, ist es sinnvoll, regelmäßig ein manuelles Update durchzuführen. Diese Vorgehensweise sollten Sie sich dann zu Eigen machen.

8.2. Das manuelle Update

Diese Methode erlaubt Ihnen, durch die Installation der neusten Virensignaturen den bestmöglichen Virenschutz zu erhalten. Für die Installation des neusten Produktupdates wählen Sie bitte das Automatische Update.

Wichtig

Bitte nutzen Sie das manuelle Update, falls das automatische Update nicht ausgeführt wurde, oder wenn der Computer nicht mit dem Internet verbunden ist.

Es gibt zwei mögliche Varianten, ein manuelles Update durchzuführen:

- Mit einer `weekly.exe` Datei;
- Mit einem `zip Archiv`.

8.2.1. Das manuelle Update mit der `weekly.exe` Datei

Das Update Paket `weekly.exe` wird jeden Freitag freigeschaltet und enthält alle neuen Virusdefinitionen und Prüfmechanismen bis zum Freigabedatum.

Um das BitDefender Update über die Datei `weekly.exe` durchzuführen, folgen Sie den nächsten Schritten:

1. Herunterladen der weekly.exe und speichern Sie diese Datei lokal auf Ihrer Festplatte.
2. Rufen Sie die herunter geladene Datei auf und mit einem Doppelklick rufen Sie den Update Assistenten auf.
3. Klicken Sie auf **Weiter**.
4. Überprüfen Sie **Ich akzeptiere die Lizenzvereinbarungen** und klicken Sie auf **Weiter**.
5. Klicken Sie auf **Installieren**.
6. Klicken Sie auf **Fertigstellen**.

8.2.2. Das manuelle Update per ZIP Archiv

Es sind zwei ZIP Archive auf dem BitDefender FTP-Servern verfügbar, die alle Virussignaturen und Püfmechanismen beinhalten: `cumulative.zip` und `daily.zip`.

- Der `cumulative.zip` wird jede Woche montags veröffentlicht und beinhaltet alle neuen Virus Definitionen und Prüfmechanismen bis zum Datum der Veröffentlichung.
- Der `daily.zip` wird jeden Tag veröffentlicht und enthält alle neuen Virus Definitionen und Prüfmechanismen ausgehend von der letzten, erfolgten Zusammenstellung bis zum heutigen Tag.

BitDefender verwendet eine servicebasierte Architektur. Aufgrund dieser Vorgehensweise ist die Erneuerung der Viren - Definitionen abhängig vom Betriebssystem:

- Windows NT 4, Windows 2000, Windows XP.
- Windows 98, Windows Millenium.

Windows NT 4, Windows 2000, Windows XP

Folgende Schritte sind notwendig:

1. **Herunterladen des richtigen Updates .** Bitte laden sie Montags das Archiv cumulative.zip herunter und speichern Sie dieses Archiv im Eingabefeld im gewünschten Verzeichnis. Ansonsten laden Sie bitte das Archiv daily.zip herunter und speichern Sie dieses Archiv ebenfalls auf dem gewünschten Festplattenverzeichnis. Falls es das erste Update ist, welches Sie manuell durchführen, laden Sie bitte beide Archive herunter.

2. Beenden der BitDefender Virusschutzfunktion

   - **Verlassen Sie bitte die BitDefender Management Konsole .** In dem Sie mit einem Rechtsklick auf das BitDefender-Symbol der System Tray klicken und **Beenden** wählen.
   - **Öffnen der Dienste .** Klicken Sie **Start** in der Taskleiste, dann **Systemsteuerung**, Doppelklick auf **Verwaltung** und dann klicken Sie **Dienste**.
   - **Stoppen des BitDefender Virus Schild .** Wählen Sie den Service **BitDefender Virus Schild** aus der angezeigten Liste und klicken sie auf **Stoppen**.
   - **Stoppen der BitDefender Scan Server .** Wählen Sie den Service **BitDefender Scan Server** aus der angezeigten Liste und klicken Sie auf **Stoppen**.

3. **Extrahieren der Archivinhalte .** Starten Sie bitte mit dem Archiv `cumulative.zip` sobald beide Archive verfügbar sind. Extrahieren Sie die Inhalte in das Verzeichnis `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` und bestätigen Sie das Überschreiben der bestehenden Dateien.

4. Neustart der BitDefender Antivirusfunktion.

   - **Starten des BitDefender Scan Server .** Wählen Sie **BitDefender Scan Server** in der angezeigten Liste und klicken Sie **Starten**.
   - **Starten des BitDefender Virus Schild .** Wählen Sie **BitDefender Virus Schild** von der angezeigten Liste und klicken Sie **Starten**.
   - Öffnen Sie BitDefender Management Konsole.

Windows NT 4, Windows 2000, Windows XP

Folgende Schritte sind notwendig:

1. **Herunterladen des richtigen Updates .** Bitte laden sie Montags das Archiv cumulative.zip herunter und speichern Sie dieses Archiv im Eingabefeld im gewünschten Verzeichnis. Ansonsten laden Sie bitte das Archiv daily.zip herunter und speichern Sie dieses Archiv ebenfalls auf dem gewünschten Festplattenverzeichnis. Falls es das erste Update ist, welches Sie manuell durchführen, laden Sie bitte beide Archive herunter.

2. **Extrahieren der Archivinhalte .** Starten Sie bitte mit dem Archiv `cumulative.zip` sobald beide Archive verfügbar sind. Extrahieren Sie die Inhalte in das Verzeichnis `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` und bestätigen Sie das Überschreiben der bestehenden Dateien.

3. Bitte starten Sie Ihren Computer neu.

8.3. Update-Einstellungen

Um diese Sektion zum öffnen, klicken Sie bitte **Einstellungen** im Modul **Update**.

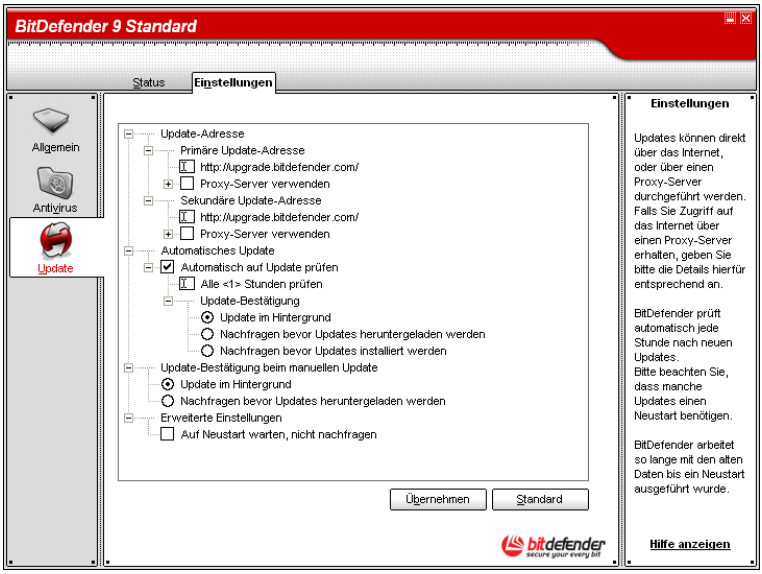


Abbildung 8.2. Update-Einstellungen

Updates können vom lokalen Netz, über das Internet, direkt oder durch einen Proxy-Server durchgeführt werden.

Das Fenster mit den Update-Einstellungen enthält 4 aufklappbare Optionskategorien (**Update-Adresse**, **Automatisches Update**, **Update-Bestätigung beim manuellen Update** und **Erweiterte Einstellungen**), ähnlich wie in den Windowsmenüs.

Anmerkung

Klicken Sie auf das Kästchen mit dem " + "-Zeichen, um eine Option zu öffnen, oder auf das "-"-Zeichen, um eine Option zu schließen.

8.3.1. Update-Adresse

Für ein zuverlässigeres Update können zwei Update-Adressen angegeben werden. Ist die **primäre Adresse** nicht erreichbar, so wird auf der **sekundären Update-Adresse** nach verfügbaren Updates gesucht. Die folgenden Optionen sind verfügbar:

- **Update-Adresse** - Befinden Sie sich in einem lokalen Netzwerk und werden Updates über einen lokalen Update-Server bereitgestellt so ist es möglich, hier eine lokale Adresse anzugeben und die Updates über das Netzwerk zu beziehen statt über das Internet. Die voreingestellte Adresse ist: http://upgrade.bitdefender.com.

- **Proxy-Server verwenden** - Falls Sie einen Proxy-Server einsetzen, muss die entsprechende Markierung gesetzt werden. Nehmen Sie dann folgende Einstellungen vor:

  - **Adresse** - Geben Sie hier die IP-Adresse oder den Hostnamen des Proxy-Serversein, den BitDefender verwendet.

    Wichtig

    Syntax: `name:port` oder `ip:port`.

  - **Benutzername** - Geben Sie den Benutzernamen ein, wenn der Proxy-Server eine Anmeldung erfordert.

Wichtig

Syntax: `domain\user`.

- **Kennwort** - Geben Sie das Kennwort ein, wenn der Proxy-Server eine Anmeldung mit Kennwort erfordert.

8.3.2. Automatisches Update

- **Automatisch auf Update prüfen** - BitDefender verbindet sich automatisch mit dem BitDefender- Update-Server und prüft, ob neue Updates vorhanden sind.
- **Alle 1 stunden prüfen** - Definiert, wie oft auf verfügbare Updates geprüft werden soll. Standard ist 1 Stunden.
- **Update im Hintergrund** - BitDefender führt Updates komplett selbständig durch.
- **Vor dem Herunterladen fragen** - BitDefender informiert den Benutzer vor dem Herunterladen der neuen Updates.
- **Vor der Installation fragen** - BitDefender informiert den Benutzer vor der Installation neuer Updates.

Wichtig

Wenn Sie die Optionen **Vor dem Herunterladen fragen** oder **Vor der Installation fragen** aktiviert haben und Sie die Management Konsole schließen und beenden, werden automatische Updates nicht durchgeführt.

8.3.3. Update-Bestätigung beim manuellen Update

- **Update im Hintergrund** - BitDefender führt Updates komplett selbständig durch.
- **Vor dem Herunterladen fragen** - BitDefender informiert den Benutzer vor dem Herunterladen der neuen Updates.

Wichtig

Wenn Sie die Optionen **Vor dem Herunterladen fragen** aktiviert haben und Sie die Management Konsole schließen und beenden, werden manuelle Updates nicht durchgeführt.

8.3.4. Erweiterte Einstellungen

- **Auf Neustart warten, nicht nachfragen** - Falls ein Update den Neustart des Computers benötigt teilt BitDefender dies mit und fragt den Benutzer ob der Neustart nun durchgeführt werden soll. Der Benutzer wird nicht gefragt, ob ein Neustart durchgeführt werden soll. Somit wird der Benutzer während der Arbeit nicht durch BitDefender unterbrochen.

Klicken Sie auf **Übernehmen** um die Veränderungen zu speichern. Durch Klicken auf **Standard** laden Sie die Standardeinstellungen.

Tipps und Tricks

Kapitel 9. Tipps und Tricks

Der Abschnitt **Tipps und Tricks** behandelt und erklärt das Thema:

- Antivirus

9.1. Antivirus

Um einen virusfreien Computer zu erzeugen, folgen Sie bitte den nächsten Schritten:

1. Wenn der Installationsprozess beendet ist, sollten Sie, wie in der Sektion *„Registrierung des Produkts“* (S. 27) beschrieben, Ihr BitDefender-Produkt registrieren.

2. Bitte führen Sie ein benutzergesteuertes Update mit den aktuellen Virensignaturen, wie in der Sektion *„Das automatische Update“* (S. 71) beschrieben, durch.

3. Wählen Sie die komplette Prozedur, wie in der Sektion *„ Sofortiges prüfen “* (S. 44) beschrieben.

4. In der Sektion Status des Modul **Allgemein** aktivieren Sie bitte die wichtigsten BitDefender Funktionen: **Virus Schild** und **Automatisches Update**.

5. Bitte richten Sie Ihren Computer so ein, dass er mindestens einmal pro Woche einen Prüfvorgang durchführt. Dies ist in der Sektion *„Prüfen mit dem BitDefender Planer“* (S. 54) nochmals beschrieben.

BitDefender Notfall CD

BitDefender 9 Standard verfügt über eine bootfähige CD-ROM (BitDefender Notfall CD basierend auf LinuxDefender), die fähig ist alle Festplatten zu prüfen und zu desinfizieren, bevor Ihr Betriebssystem startet.

Sie sollten die BitDefender Rescue CD immer dann verwenden, wenn Ihr System aufgrund von Virusinfektionen nicht mehr richtig funktioniert. Dies passiert für gewöhnlich, wenn Sie kein Antivirus-Programm benutzen.

Das Update der Virensignaturen wird automatisch ohne Benutzereingriff jedes Mal vollzogen, wenn Sie die BitDefender Rescue CD starten.

Kapitel 10. Übersicht

LinuxDefender ist eine, mit BitDefender erweiterte, Knoppix-Distribution, welche die neueste Version von BitDefender für Linux in das GNU/Linux integriert. Es beinhaltet einen SMTP Antivirus/Antispam-Schutz und einen On Demand Scanner, der in der Lage ist Festplatten (inkl. Windows NTFS-Partition), Samba-Freigaben und NFS Mount Points zu überprüfen und zu desinfizieren. Eine web-basierende Konfigurationsschnittstelle zu den BitDefender-Lösungen ist ebenfalls enthalten.

Aktuelle Bestandteile

- Direkte Überprüfung von E-Mails (Antivirus & Antispam)
- Antivirus-Lösungen für Ihre Festplatten
- NTFS Schreib-Unterstützung (über Captive-Projekt)
- Desinfektion infizierter Dateien von Partitionen unter Windows XP (NTFS)

10.1. Was ist Knoppix?

Auszug aus http://knopper.net/knoppix:

„ KNOPPIX ist eine komplett von CD oder DVD lauffähige Zusammenstellung von GNU/Linux (http://www.linux.com) Software mit automatischer Hardwareerkennung und Unterstützung für viele Grafikkarten, Soundkarten, SCSI- und USB-Geräte und sonstige Peripherie. KNOPPIX kann als produktives Linux-System für den Desktop, Schulungs-CD, Rescue-System oder als Plattform für kommerzielle Software-Produktdemos angepasst und eingesetzt werden. Es ist keinerlei Installation auf Festplatte notwendig. “

10.2. Systemanforderungen

Bevor Sie LinuxDefender booten stellen Sie bitte sicher, dass Ihr System die folgenden Vorraussetzungen erfüllt.

Prozessortyp	X86 kompatibel mit einem Minimum von 166 MHz, aber bitte erwarten Sie in diesem Falle keine zufrieden stellende Systemleistung. Eine i686 Prozessorgeneration mit 800MHz wäre die bessere Wahl.
Speicher	Die mindestens benötigte Speichergröße liegt bei 64MB, für eine bessere Systemleistung wird jedoch 128 MB empfohlen.
CD-ROM	CD-Rom-Laufwerk und die BIOS-Einstellungen um von CD zu booten.
Internetverbindung	Obwohl LinuxDefender auch ohne Internetverbindung lauffähig ist, benötigen die Update-Vorgänge eine aktive HTTP-Verbindung oder durch einen Proxy Server. Daher ist für einen aktuellen Schutz eine Internetverbindung ein MUSS.
Grafische Auflösung	800x600 für die web-basierende Administration.

10.3. Integrierte Software

Die Bitdefender Notfall CD enthält die folgenden Software-Pakete.

- BitDefender SMTP Proxy (Antispam & Antivirus)
- BitDefender Remote Admin
- BitDefender Linux Edition (Antivirus) + GTK Interface
- BitDefender Documentation (PDF- & HTML-Format)
- BitDefender Extras (Artwork, Leaflets)
- Linux-Kernel 2.6
- Captive NTFS write project
- LUFS - Linux Userland File System
- Werkzeuge zur Datenwiederherstellung
- Netzwerk- und Sicherheits-Analyse Werkzeuge für Administratoren
- Amanda Backup Lösung
- thttpd Tiny HTTP Daemon (Web-Server)
- Ethereal & Nessus (Netzwerkdatenverkehrs-Analyse)
- Parted, QTParted und Partimage (Partitionierungs-Werkzeuge)
- Adobe Reader (Zur Anzeige von PDF-Dokumenten)
- Mozilla Firefox Web browser

10.4. BitDefender Lösungen auf dieser CD-ROM

Die LinuxDefender Notfall CD beinhaltet die BitDefender SMTP Proxy Lösung für Linux mit integriertem Antivirus/Antispam, BitDefender Remote Admin (einer web-basierenden Verwaltungsoberfläche) und einer BitDefender Linux Edition (On-Demand Kommandozeilen-Scanner).

10.4.1. BitDefender SMTP Proxy

BitDefender für Linux Mail Server – SMTP Proxy ist eine Content-Inspection-Lösung, welche neben dem Schutz vor Viren zusätzlich Antispam-Funktionalitäten beinhaltet. Beide Schutzvarianten arbeiten direkt auf Gateway-Ebene, um somit den gesamten E-Mail-Datenverkehr überprüfen und effektiv sichern zu können. Durch die Verwendung fortschrittlichster Technologien ist BitDefender für Linux Mail Server mit allen gängigen E-Mail-Servern kompatibel und erhielt außerdem die Zertifizierung „Red Hat Ready".

Die Antivirus- und Antispam-Lösungen überprüfen, desinfizieren und filtern E-Mails auf allen gängigen E-Mail-Servern und auf nahezu jeder Betriebssystem-Plattform. BitDefender für Linux Mail Server – SMTP Proxy wird direkt beim Bootvorgang gestartet und überprüft alle eingehenden E-Mails. Um das Produkt zu konfigurieren, kann BitDefender Remote Admin, eine web-basierende Konfigurationsschnittstelle, verwendet werden.

10.4.2. BitDefender Remote Admin

Die BitDefender-Dienste können sowohl lokal als auch extern verwaltet werden. Gehen Sie hierzu bitte wie folgt vor:

1. Starten Sie den Firefox Web-Browser und öffnen Sie die Internetadresse : https://localhost:8139 (oder klicken Sie bitte doppelt auf das BitDefender Remote Admin Symbol auf Ihrem Desktop)
2. Melden Sie sich mit dem Benutzer „bd" und dem Kennwort „bd" am System an
3. Wählen Sie „SMTP Proxy" aus dem linken Menü
4. Tragen Sie den „echten" SMTP-Server und den Port ein
5. Fügen Sie E-Mail-Domains zum Relaying hinzu
6. Fügen Sie Netzwerk-Domains zum Relaying hinzu

7. Wählen Sie „Antispam“ aus dem linken Menü aus, um diese Funktionalität zu konfigurieren
8. Wählen Sie „Antivirus““ aus dem linken Menü aus, um diese Funktionalität zu konfigurieren
9. Zusätzlich können Sie per „Mail Notifications“ die Benachrichtigungen konfigurieren

10.4.3. BitDefender Linux Edition

Der Antiviren-Scanner von BitDefender Linux Edition integriert sich direkt auf den Linux Desktop. Diese Version des Produkts beinhaltet eine auf GTK+ basierende grafische Benutzeroberfläche, über die der Prüfvorgang durchgeführt werden kann.

Wählen Sie in der Benutzeroberfläche einfach den zu überprüfenden Pfad bzw. das Laufwerk aus und klicken Sie mit der rechten Maustaste auf das jeweilige Objekt. Wählen Sie nun aus dem Kontextmenü den Eintrag „Scan with BitDefender“. Der Prüfvorgang wird nun gestartet und der Status des Prüfvorgangs inkl. einem abschließendem Bericht wird angezeigt. Für die Option Feineinstellungen lesen Sie bitte in der Linux Edition Dokumentation (in dem BitDefender Verzeichnis für Dokumentation oder entsprechenden Handbuchseite) und dem **/opt/BitDefender/lib/bdc** Programm nach.

Kapitel 11. LinuxDefender Kurzanleitung

11.1. Starten und Beenden

11.1.1. LinuxDefender starten

Um von der CD-ROM starten zu können, müssen Sie zunächst das BIOS Ihres Computers so konfigurieren, dass die Bootreihenfolge folgendermaßen aussieht:CD-ROM Laufwerk, Floppy-Laufwerk, Festplatte.

Starten Sie nun Ihren Computer neu und warten Sie, bis der Initiale Bootvorgang abgeschlossen wurde. Sie bekommen nun den LinuxDefender Startbildschirm angezeigt. Folgen Sie nun bitte den angegebenen Schritten, um LinuxDefender zu starten.

Abbildung 11.1. LinuxDefender Startbildschirm

Drücken Sie F2 um die erweiterten Einstellungen anzuzeigen. Drücken Sie bitte die Taste F3 für die erweiterten Einstellungen in deutscher Sprache. Drücken Sie bitte die Taste F4 für die erweiterten Einstellungen in französische Sprache. Drücken Sie bitte die Taste F5 für die erweiterten Einstellungen in spanische Sprache. Um das System direkt zu starten, drücken Sie bitte die Taste ENTER.

Sobald der Bootvorgang abgeschlossen wurde, wird der LinuxDefender Desktop angezeigt. Sie können nun damit beginnen, LinuxDefender zu verwenden.

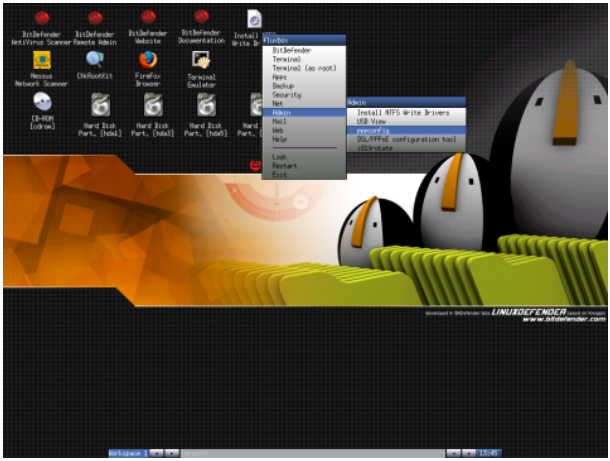


Abbildung 11.2. Der LinuxDefender Desktop

11.1.2. LinuxDefender beenden

Um LinuxDefender ordnungsgemäß zu beenden, empfehlen wir die folgende Vorgehensweise: Klicken Sie per Rechtsklick auf das jeweiligen Festplatten-Symbol auf dem Desktop und wählen Sie **umount** aus dem Kontextmenü. Klicken Sie nun mit der rechten Maustaste auf eine freie Stelle auf dem Desktop und wählen Sie aus dem Kontextmenü den Befehl **Exit**.

Abbildung 11.3. Wählen Sie "EXIT"

Sobald LinuxDefender alle Programme beendet hat, bekommen Sie eine textbasierte Ausgabe angezeigt. Sobald der Satz **Please remove CD, close cd-rom drive and hit return** angezeigt wird, können Sie die CD aus dem Laufwerk entfernen, den Einschub schließen und die Taste **ENTER** betätigen. Der Computer wird nun neu gestartet und Ihr bevorzugtes Betriebssystem gestartet.

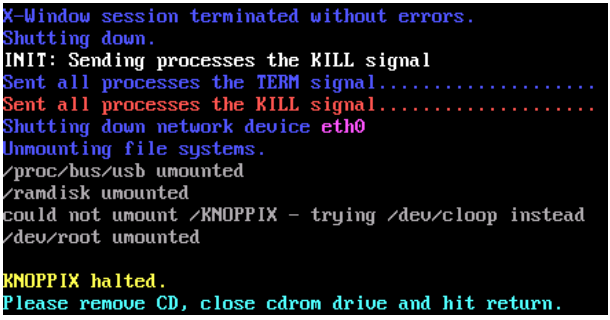

X-Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Sent all processes the TERM signal.....
Sent all processes the KILL signal.....
Shutting down network device eth0
Unmounting file systems.
/proc/bus/usb umounted
/ramdisk umounted
could not umount /KNOPPIX - trying /dev/cloop instead
/dev/root umounted
KNOPPIX halted.
Please remove CD, close cdrom drive and hit return.

Abbildung 11.4. Warten auf diese Nachricht, wenn der Rechner heruntergefahren wird

11.2. Internetverbindung konfigurieren

Falls Sie über ein Netzwerk mit DHCP-Funktionalität verfügen und eine Netzwerkkarte in Ihrem Computer installiert ist, sollte LinuxDefender die notwendigen Einstellungen automatisch erkennen. Für eine manuelle Konfiguration folgen Sie bitte den folgenden Schritten.

1. Öffnen Sie per Rechtsklick auf den Desktop das Kontextmenü und wählen Sie **Terminal**.
2. Geben Sie **netcardconfig** als Befehl ein und drücken Sie die Taste **ENTER**.
3. Falls Sie DHCP in Ihrem Netzwerk verwenden, wählen Sie bitte **yes**.
4. Die Netzwerkkonfiguration sollte nun automatisch erkannt werden. Mit dem **ifconfig** können Sie Ihre IP Adresse and Netwerkkarteneinstellungen einsehen.
5. Falls Sie eine statische IP-Adresse verwenden (kein DHCP), wählen Sie stattdessen **No**.
6. Folgen Sie den Instruktionen auf dem Bildschirm und konsultieren Sie Ihren Administrator.

Sollten diese Schritte erfolgreich abgeschlossen haben, können Sie die Verbindung folgendermaßen überprüfen. Geben Sie dazu den Befehl in das Terminal ein und drücken Sie ENTER.

```
$ ping -c 3 bitdefender.com
```

Sie erhalten nun eine Ausgabe mit den Antwortzeiten unsere Server (falls die Konnektivität besteht), oder eine Meldung ähnlich „Host is down“ bzw. „No route to host“ falls keine Konnektivität besteht

Falls Sie eine Einwahlverbindung verwenden, wählen Sie bitte **pppconfig** vom LinuxDefender Administrationsmenü. Folgen Sie bitte dann den Bildschirminstruktionen, um die PPP Internet Verbindung einzustellen.

11.3. BitDefender per Update aktualisieren

Die BitDefender Pakete für die LinuxDefender verwenden den Festplattenspeicher des Systems für erneuerbare Dateien. Über diesen Weg können Sie die neuen Virensignaturen, Prüfmaschinen, oder die AntiSpam Datenbank aktualisieren. Dies

geschieht sogar, wenn das System über Read only Medien, wie z.B. LinuxDefender CD arbeitet.

Stellen Sie bitte zunächst sicher, ob Ihre Internetverbindung funktioniert. Öffnen Sie nun BitDefender Remote Admin und wählen Sie im linken Menü **Live! Update**. Klicken Sie nun auf die Schaltfläche **Update Now**, um das Update durchzuführen.

Alternativ können Sie auch ein Update über das Terminal durchführen. Dazu verwenden Sie bitte den folgenden Befehl.

```
# /opt/BitDefender/bin/bd  update
```

Sämtliche Updatevorgänge werden in einer Berichtsdatei protokolliert. Diese können Sie mit dem folgenden Befehl im Terminal einsehen.

```
# tail  -f /ramdisk/BitDefender/var/log/bd.log
```

Falls Sie einen Proxy-Server zum Herstellen einer Internetverbindung verwenden, müssen Sie diesen Server zunächst im BitDefender Remote Admin, im Bereich **Live! Update** über die Schaltfläche **Configuration** angeben.

11.4. Prüfvorgänge durchführen

11.4.1. Wie erhalte ich Zugriff auf meine Daten unter Windows?

NTFS Schreibzugriff

Der NTFS Schreibzugriff wird über das Captive NTFS Projekt realisiert. Um diesen Zugriff zu verwenden benötigen Sie die folgenden Dateien Ihrer Windows-Installation: `ntoskrnl.exe` und `ntfs.sys`. Derzeit werden nur Windows XP Treiber unterstützt. Sie können diese Treiber jedoch auch dazu verwenden, um auf Partitionen von Windows NT 4.0, 2000 und 2003 zu zugreifen. Für Windows 98 und Me werden keinerlei Treiber zum Schreibzugriff benötigt.

Installieren der NTFS Treiber

Um einen Zugriff zu Ihren Windows-Partitionen mit NTFS-Dateisystem zu erhalten und auf diesen schreiben zu können, müssen Sie zunächst die NTFS Treiber installieren. Wird dieser Schritt nicht durchgeführt, erhalten Sie nur schreibgeschützten Zugriff. Falls Sie FAT und nicht NTFS für Ihre Windows Partitionen verwenden, oder lediglich einen Lesezugriff für Ihre Daten benötigen, können Sie die Laufwerke direkt einbinden und somit einen Zugriff auf Windows Laufwerke erhalten, als wären es Linux Laufwerke.

Um die Schreibunterstützung zu erhalten, speichern Sie die NTFS Treiber auf Ihrer lokalen Festplatte, entfernte Netzlaufwerke, einen USB Stick oder beziehen Sie diese Treiber direkt über das Windows Update. Es wird empfohlen, nicht die Treiber der verwendeten Windows-Installation einzusetzen, da diese im Falle einer Infizierung durch einen Virus ggf. ebenfalls beschädigt sind und nicht korrekt funktionieren.

Klicken Sie doppelt auf das Desktop-Symbol **Install NTFS Write Drivers**, um den Installationsvorgang zu starten. Wählen Sie die erste Option, wenn Sie die Treiber von der lokalen Festplatte installieren möchten.

Haben Sie die Treiber an einem anderen Ort gespeichert, wählen Sie bitte **Quick search** aus, um nach den Treiber suchen zu lassen.

Alternativ können Sie selbst einen Speicherort angeben, oder die Treiber direkt über den Download des Service Pack 1 für Windows XP beziehen.

Die Treiber werden nicht auf Ihrer Festplatte installiert, sondern lediglich temporär von LinuxDefender verwendet, um auf die NTFS-Partitionen zu zugreifen. Sofern das Programm die Treiber installiert hat, können Sie die entsprechenden Partition per Doppelklick aufrufen und deren Inhalt einsehen. Für einen wirkungsvollen Datei Manager verwenden Sie bitte den Midnight Commander von dem LinuxDefender Menü (oder geben Sie **mc** in der Konsole ein).

11.4.2. Wie führe ich einen Prüfvorgang durch?

Wählen Sie die gewünschten Ordner aus und klicken Sie per Rechtsklick auf diese. Wählen Sie nun aus dem Kontextmenü den Eintrag **Send to** und klicken Sie nun auf **BitDefender Scanner**.

Alternativ kann der Prüfvorgang auch mit Rechten des Benutzers root über den Terminal durchgeführt werden. Geben Sie dazu den folgenden Befehl im Terminal ein und bestätigen Sie mit der Taste ENTER.

```
# /opt/BitDefender/bin/bdgtk2 /path/to/scan/
```

Klicken Sie nun in der Benutzeroberfläche auf **Start Scan**.

Falls Sie weitere Einstellungen vornehmen möchten, klicken Sie zuvor bitte auf **Configure Antivirus**.

11.5. Erstellen einer Ad-Hoc Mail-Filterungs-Lösung

Sie können LinuxDefender dazu benutzen, eine Ad-Hoc Mail-Filter-Lösung zu erstellen, ohne dass Sie eine Software installieren oder den E-Mail-Server modifizieren müssen. Die Idee dahinter ist, dass Sie ein LinuxDefender System vor Ihrem Mail-Server benutzen und BitDefender erlauben, jeden SMTP-Verkehr nach Spam und Viren zu scannen und ihn anschließend gefiltert an den Mail-Server weiterzugeben.

11.5.1. Vorbereitende Maßnahmen

Sie benötigen mindestens einen Computer mit einer Pentium 3-kompatiblen CPU, 256MB RAM und ein CD/DVD-Laufwerk, um davon zu starten. LinuxDefender muss den SMTP-Verkehr statt dem eigentlichen E-Mail-Server bekommen. Es gibt verschiedene Wege um dies einzustellen.

1. Ändern Sie die IP des eigentlichen Mail-Servers und vergeben die alte IP an das LinuxDefender System
2. Ändern Sie Ihre DNS-Einträge, sodass der MX-Eintrag für Ihre Domains zu dem LinuxDefender System zeigt
3. Stellen Sie Ihre Mail-Clients auf das neue LinuxDefender System als SMTP-Server ein
4. Ändern Sie Ihre Firewall-Einstellungen so ab, dass alle SMTP-Serververbindungen an LinuxDefender weitergeleitet werden, anstatt an den eigentlichen Mail-Server

Das Linux How To wird die obigen Anweisungen nicht Erklären. Für weitere Informationen konsultieren Sie bitte Linux Networking guides und Netfilter documentation.

11.5.2. Der Mail-Filter

Starten Sie Ihre LinuxDefender CD-ROM und warten Sie, bis das X Window-System geladen ist.

Um den BitDefender SMTP-Proxy zu konfigurieren, doppelklicken Sie auf das **BitDefender Remote Admin** Symbol auf dem Desktop. Das folgende Fenster wird erscheinen. Benutzen Sie als Benutzernamen und als Kennwort `bd`, um sich anzumelden.

Nach dem erfolgreichen Login bekommen Sie die Möglichkeit den BitDefender SMTP-Proxy zu konfigurieren.

Wählen Sie **SMTP Proxy** aus, um den eigentlichen Mail-Server, den Sie vor Viren und Spam schützen möchten.

Klicken Sie auf die Kategorie **Email domains**, um alle Domains einzugeben, von denen Sie E-Mails akzeptieren möchten.

Wählen Sie **Add Email Domain** oder **Add Bulk Domains** und folgen den Anweisungen um die Relays einzustellen.

Wählen Sie die Kategorie **Net domains** um alle Netzwerke einzugeben, die Sie relayen möchten.

Wählen Sie **Add Net Domain** oder **Add Bulk Net Domains** und folgen den Anweisungen um die Relays einzustellen.

Wählen Sie **Antivirus** aus dem linken Menü, um auszuwählen was zu tun ist, wenn ein Virus gefunden wird, und um andere Antivirus-Optionen zu konfigurieren.

Nun wird der gesamte SMTP-Verkehr von BitDefender gescannt und gefiltert. Standardmäßig werden alle virusinfizierte Mails gesäubert und alle Spam E-Mails von BitDefender werden im Betreff der Mail mit dem Wort `[SPAM]` gekennzeichnet. Ein E-Mail-Header (`X-BitDefender-Spam: Yes/No`) wird zu jeder Mail hinzugefügt, um die client-seitige Filterung zu erleichtern.

11.6. Eine Netzwerk-Sicherheitsprüfung durchführen

Neben den Möglichkeiten der Erkennung von Schädlingen und dem Filtern von E-Mails ist es mit LinuxDefender auch möglich, Ihr Netzwerk einer Sicherheitsprüfung zu unterziehen. Für diesen Fall sind Computer-forensische Werkzeuge auf dieser CD-ROM enthalten, mit denen es möglich ist, kompromittierte Systeme zu überprüfen und das Netzwerk auf Eindringlinge zu untersuchen. Bitte lesen Sie diese kurze Einführung, um mehr darüber zu erfahren, wie man eine kurze Prozessanalysen der Server und des Netzwerks vornimmt.

11.6.1. Auf Rootkits überprüfen

Bevor Sie Ihr Netzwerk einer solchen Prüfung unterziehen, sollten Sie zunächst sicherstellen, dass der Host, von dem Sie die Prüfung durchführen, nicht kompromittiert wurde. Starten Sie hierfür zunächst einen Prüfvorgang mit BitDefender. Sie können einen Prüfvorgang für die installierten Festplatten vornehmen, beschrieben in der Einführung für **Prüfen auf Viren** , oder Sie können auf Unix rootkits (ähnlich zu trojanischen Pferden) prüfen.

Überprüfen Sie nun, ob eventuelle Eindringlinge einen Rootkit (eine Art Hintertür) auf dem System installiert haben. Zu diesem Zwecke wird das Programm **ChkRootKit** mitgeliefert. Um bestimmte Festplatten mittels diesem Programm zu überprüfen, verwenden Sie bitte den folgenden Befehl im Terminal und bestätigen Sie diesen anschließend mit der Taste ENTER.

```
# chkrootkit -r /dev/hda3
```

Wird ein Rootkit gefunden, so zeigt das Programm diese Ausgabe in **fetter Schrift** im Terminal an.

11.6.2. Nessus – der Netzwerk Scanner

Was ist Nessus? „ Nessus ist die beliebteste Open-Source Software zum Entdecken von Sicherheitslücken in Netzwerken und wird von über 75.000 Unternehmen weltweit eingesetzt. “

Nessus kann dazu eingesetzt werden, das Netzwerk entfernt auf verschiedenste Sicherheitslücken zu überprüfen und schlägt diverse Verbesserungsvorschläge vor, um das Netzwerk zu sichern und das Risiko eines Einbruchs zu minimieren.

Klicken Sie doppelt auf das Desktop-Symbol **Nessus Security Scanner**, oder starten Sie das Programm über den Befehl **startnessus** im Terminal. Warten Sie nun bis das Fenster angezeigt wird. Dies kann je nach Hardware-Konfiguration 5 bis 10 Minuten andauern, da die Software über 5.000 Plug-Ins beinhaltet. Verwenden Sie den Benutzer `knoppix` und das Kennwort `knoppix` um sich anzumelden.

Klicken Sie auf den Abschnitt **Target selection** und geben Sie die IP-Adressen bzw. Hostnamen der Computer an, die Sie auf möglichre Sicherheitslücken überprüfen möchten. Stellen Sie danach sicher, dass die Prüfoptionen gemäß den Gegebenheiten in Ihrem Netzwerk angepasst sind. Somit können Sie Ressourcen und Bandbreite einsparen und erhalten ein akkurateres Prüfergebnis. Klicken Sie nun auf **Start the scan** um den Prüfvorgang zu starten.

Nach Abschluss des Prüfvorgangs erhalten Sie einen ausführlichen Bericht des Programms angezeigt, welcher Sie auf Schwachstellen hinweist und entsprechende Empfehlungen zu diesen bereitstellt. Der gespreicherte Bericht kann in dem von Ihnen bevorzugten Browser eingesehen werden.

11.7. Den RAM Ihres Computers überprüfen

Sollte Ihr Computer des Öfteren unerwartet abstürzen oder sog. „Blue Screens“ anzeigen, empfehlen wir Ihnen, den Arbeitsspeicher (RAM) Ihres Computers zu überprüfen. Dies können Sie ebenfalls mittels der LinuxDefender Rescue CD durchführen. Gehen Sie hierzu bitte wie folgt beschrieben vor.

Starten Sie Ihren Computer von der LinuxDefender CD und warten Sie bis die den Startbildschirm mit erweiterten Einstellungsmöglichkeiten angezeigt bekommen. Tippen Sie nun den Befehl **memtest** ein und bestätigen Sie diesen mit drücken der Tast ENTER.

Das Programm zum Überprüfen des Arbeitsspeichers startet nun automatisch und überprüft diesen in mehreren Durchgängen. Sie können die Einstellungen des Speichertests jederzeit durch Drücken der Taste C auf Ihrer Tastatur beliebig anpassen.

Ein vollständiger Test des Arbeitsspeichers benötigt circa 8 Stunden, abhängig von der Kapazität und Geschwindigkeit des Speichers. Es wird empfohlen diesen Test komplett durchlaufen zu lassen, er kann jedoch jederzeit durch drücken der Taste ESC auf Ihrer Tastatur abgebrochen werden.

Falls Sie vor kurzem neuen Arbeitsspeicher erworben haben, empfehlen wir Ihnen diesen einmal mittels dieser Methode zu überprüfen, um eventuelle Produktionsfehler noch vor Ablauf der Garantie zu erkennen und somit Systemabstürze und Datenverlust zu vermeiden.

Getting help

Kapitel 12. Support

12.1. Technische Beratung

Als eines der führenden Dienstleistungsunternehmen für IT Sicherheitslösungen möchten wir Ihnen eine möglichst schnelle, kompetente und unkomplizierte technische Unterstützung bei auftretenden Fragen anbieten. Unser technischer Support ist zu diesem Zweck stets mit den aktuellsten Virensignaturen, neusten Informationen und präzisen Antworten auf wiederkehrende Fragen ausgestattet.

Insbesondere zeichnet sich SOFTWIN durch ein hohes Maß an Innovation, ein hervorragendes Preis-Leistungsverhältnis und eine kurze Reaktionszeit in allen Belangen aus. Kundenzufriedenheit ist für uns nicht nur eine Floskel, sondern Firmenphilosophie. Es ist jedoch leider nicht vollkommen auszuschließen, dass es bei der Bearbeitung Ihrer Anfragen zu Engpässen kommen kann und bitten diesbezüglich um Nachsicht.

Wir freuen uns auf die Kontaktaufnahme zu unseren technischen Support und stehen Ihnen mit Rat und Tat zur Seite. Nutzen Sie hierfür einfach unseren E-Mail Kontakt <support@bitdefender.de> , oder rufen Sie uns werktags unter (075 42) 94 44-60 kostenfrei an. Falls Sie den Weg über E-Mail bevorzugen, teilen Sie uns bitte mit, welches Produkt und Betriebssystem Sie verwenden und beschreiben Sie das aufgetretene Problem so detailliert als möglich.

12.2. Online-Hilfe

12.2.1. BitDefender Knowledge Base

Bei der BitDefender Knowledge Base handelt es sich um eine Wissensdatenbank mit Informationen und hilfreichen Tipps & Tricks rund um die BitDefender Produkte. In leicht zugänglicher Form bietet die Knowledge Base Informationen, Anleitungen und

Berichte über neue Patches und behobene Probleme. Ebenfalls enthalten sind empfohlene Vorgehensweisen bei der Verwendung von BitDefender Produkten und allgemeine Informationen wie z.B. Präventionsmaßnahmen vor Viren und anderen Schädlingen.

Die BitDefender Knowledge Base ist zudem öffentlich zugänglich und komplett durchsuchbar. Durch diese Art der Informationsbereitstellung bieten wir unseren Kunden eine weitere Möglichkeit, technische Grundlagen und Fachwissen über unsere Produkte zu erlangen.

Die BitDefender Knowledge Base jederzeit unter der Internet-Adresse http://kb.bitdefender.de erreichbar.

12.3. Kontaktinformationen

Effiziente und kundenorientierte Kommunikation ist der Schlüssel zu einem erfolgreichen Geschäftsmodell. Seit mehr als 10 Jahren überbietet SOFTWIN konstant die bereits hochgesteckten Erwartungen unserer Kunden und Partner und diese Tradition wollen wir auch in Zukunft fortführen.

12.3.1. Kontaktadressen

Technische Beratung: <support@bitdefender.de>
Virus-Einsendungen: <virus_submission@bitdefender.com>
Spam-Einsendungen: <spam_submission@bitdefender.com>
Webseite: http://www.bitdefender.de
BitDefender Knowledge-Base: http://kb.bitdefender.de

12.3.2. Adresse

Germany

Softwin GmbH
Karlsdorfer Straße 56 88069
Tettnang

Technischer Support: <support@bitdefender.de>
Vertrieb: <vertrieb@bitdefender.de>
Phone: 07542/94 44 44
Fax: 07542/94 44 99
Product web site: http://www.bitdefender.de

Spain

Constelación Negocial, S.L
C/ Balmes 195, 2ª planta, 08006
Barcelona
Soporte técnico: <soporte@bitdefender-es.com>
Ventas: <comercial@bitdefender-es.com>
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

U.S.A

BitDefender LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33308
Technical support: <support@bitdefender.us>
Sales: <sales@bitdefender.us>
Phone: 954 776 62 62, 800 388 80 62
Fax: 954 776 64 62, 800 388 80 64
Product web site: http://www.bitdefender.us

Romania

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest
Technical support: <suport@bitdefender.ro>
Sales: <sales@bitdefender.ro>
Phone: +40 21 2330780

Fax: +40 21 2330763
Product web site: http://www.bitdefender.ro

Kapitel 13. Häufig gestellte Fragen

13.1. Allgemein

F: Wie kann ich überprüfen ob BitDefender aktiviert ist?

A: Klicken Sie auf **Allgemein** und dort auf den Reiter Status. Sie sehen, welche Module von BitDefender aktiviert sind und welche nicht.

F: Welche Anforderungen an das System stellt BitDefender?

A: Zu finden im Abschnit *„Systemanforderungen“* (S. 3).

F: Wie deinstalliere ich BitDefender?

A: Der Vorgang zum Entfernen ist im Abschnitt *„Ändern, Reparieren, Deinstallation“* (S. 7)beschrieben.

F: Wie kann ich BitDefender registrieren?

A: Der Registrierungs-Vorgang ist im Abschnitt *„Registrierung des Produkts“* (S. 27)beschrieben.

13.2. Antivirus

F: Wie kann ich einen Prüfvorgang starten?

A: Klicken Sie auf **Antivirus** und wählen Sie dort den Reiter Prüfen. Wählen Sie **Lokale Laufwerke** und klicken Sie nun auf **Prüfen**.

F: Wie oft sollte ich meinem Computer prüfen?

A: Wir empfehlen den Computer mindestens einmal pro Woche zu prüfen.

F: Wie kann ich heruntergeladene Dateien automatisch prüfen?

A: BitDefender überprüft sämtliche Dateien in Echtzeit. Alles, was Sie tun müssen, ist das Virus-Schild aktiviert zu lassen.

F: Wie kann ich BitDefender anweisen periodische Prüfungen durchzuführen?

A: Klicken Sie auf **Antivirus** und dort auf den Reiter Planer. Klicken Sie nun auf **Neu** und folgen Sie dem Assistenten.

F: Was kann ich mit Dateien innerhalb der Quarantäne tun?

A: Sie können diese Dateien an das BitDefender-Virus-Labor übersenden, zuvor müssen Sie jedoch die E-Mail-Einstellungen definieren, indem Sie im Reiter Quarantäne auf **Einstellungen** klicken.

13.3. Update

F: Wieso ist es notwendig BitDefender zu aktualisieren?

A: Bei jedem durchgeführten Update werden neue Virensignaturen zum prüft Maschinen hinzugefügt hinzugefügt.

F: Wie kann ich BitDefender aktualisieren?

A: BitDefender prüft in der Standard-Einstellung alle 1 Stunden auf verfügbare Updates. Dieses Intervall können Sie unter Update verändern oder auch ein manuelles Update durchführen.

Wörterbuch

Adware

Adware ist häufig mit einer Absenderanwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware Anwendungen müssen in der Regel installiert werden, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt und somit liegt keine Rechtswidrigkeit vor.

Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren war.

AktiveX

AktiveX ist ein Programmuster, das von anderen Programmen und Betriebssystemkomponenten unter Windows aufgerufen werden kann. Die AktiveX Technologie wird von Microsofts Internet Explorer benutzt, damit interaktive Webseiten eher wie Programme und nicht wie statische Seiten angezeigt werden. Mit AktiveX können die Benutzer z.B. Fragen stellen oder beantworten, Buttons verwenden, oder verschiedenartige Interaktionen mit der Webseite herstellen. AktiveX Controls werden oft in Visual Basic geschrieben.

Erwähnenswert ist, dass bei AktiveX die Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, AktiveX über das Internet zu nutzen.

Arbeitsspeicher

Interne Speicherzonen im Rechner. Der Begriff Arbeitsspeicher bedeutet Datenträger in Form von sehr schnellen Chips, das Wort Speicher ist der Speicherplatz, der sich auf Magnetbändern oder Datenträgern befindet. Jeder Rechner hat eine

gewisse Menge Arbeitsspeicher. Dieser wird auch Hauptspeicher oder RAM genannt.

Archiv

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einer Datensicherung/BackUp erzeugt wurden.

Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.

Backdoor (Hintertür)

Eine Sicherheitslücke eines Systems, die der Entwickler oder Verwalter absichtlich hinterlässt. Der Grund dafür muss nicht immer bösartig sein. Manche Betriebssysteme haben schon bei der Fabrikation privilegierte Konten, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

Befehlzeile

Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen, die sich aus einzelnen Buchstabenfolgen zusammensetzen, statt. Als Eingabegerät wird eine Tastatur benutzt. Die Verwendung einer Maus ist nicht möglich. Auf der Befehlszeile werden die einzelnen Anweisungen in einer bestimmten Befehlssprache eingegeben, die vom Computer und seiner Software ausgewertet und mit den entsprechenden Ergebnissen auf dem Ausgabegerät (meistens ein Monitor) wieder an den Benutzer übergeben werden.

Bootsektor

Der erste Sektor einer Festplatte oder Diskette. Hier liegen Daten die das Betriebssystem zum Booten (Starten) braucht.

Bootvirus

Ein Virus, der den Bootsektor einer Festplatte oder eines Diskettenlaufwerks infiziert. Beim Versuch von einer Diskette, die mit einem Bootvirus infiziert ist, zu booten wird dieser im Arbeitsspeicher aktiviert. Bei jedem Neustart wird der Virus so im Arbeitsspeicher aktiviert und überträgt sich auf eingelegte Wechselmedien.

Browser

Kurzform für Web-Browser, eine Softwareanwendung, die zum Lokalisieren und Anzeigen von Webseiten verwendet wird. Die bekanntesten Browser sind Netscape Navigator

und Microsoft Internet Explorer. Beide sind graphische Browser, das heißt sie können sowohl Grafiken als auch Texte anzeigen. Weiterhin können die meisten Browser Multimedia-Informationen wie Klang- und Videodateien anzeigen, wobei sie für diverse Formate Plug-Ins (Zusätzliche Softwarekomponenten) benutzen.

Cookie

In der Internetindustrie werden Cookies als kleine Dateien beschrieben, die Daten über einzelne Computer enthalten und die von den Werbern analisiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden. Die Cookie-Technologie wurde deshalb weiter entwickelt, damit der Benutzer nur solche Werbung zugeschickt bekommt, die seinen Interessen dient. Für viele ist es aber wie ein zweischneidiges Messer. Einerseits ist es wirksam und sachbezogen, da man nur Anzeigen, an denen man interessiert ist, betrachten kann, anderseits heißt es dem Benutzer "auf die Spur zu kommen" und ihn auf Schritt und "Klick " zu verfolgen. Es ist verständlich, dass der Datenschutz ein umstrittenes Thema ist und viele sich von dem Begriff als SKU-Nummern (die Streifencodes auf den Packungen, die im Geschäft an der Theke gescannt werden) betrachtet zu werden, angegriffen fühlen. Auch wenn dieser Gesichtspunkt extrem erscheint ist er manchmal korrekt.

Dateierweiterung

Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind.

:call CVScommit() Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS, MS-DOS. Sie enthalten gewöhnlich ein bis zwei Buchstaben (alte Betriebssysteme können nicht mehr als drei Buchstaben unterstützen), Beispiele dafür sind "c" für C-Quellcode, "ps" für PostScript oder "txt" für beliebige Texte. Windows zeigt bei ihm bekannten Dateitypen keine Dateierweiterung in der graphischen Benutzeroberfläche an, stattdessen wird häufig ein Symbol verwendet.

Download (Herunterladen)

Kopiert Daten (gewöhnlich eine ganze Datei) von einer Hauptquelle auf ein Peripheriegerät. Der Begriff bezeichnet

	oft den Kopiervorgang von einem Online Service auf den eigenen Rechner. Download oder Herunterladen kann auch das Kopieren einer Datei von einem Netzwerkserver auf einen Netzwerkrechner bedeuten.
E-mail	Elektronische Post. Ein Dienst, der Nachrichten an andere Rechner über ein lokales oder ein globales Netzwerk übermittelt.
Ereignis	Ereignisse oder Erscheinungen, die in einem Programm vorkommen. Ereignisse können Benutzeraktionen, wie zum Beispiel Mausklicks oder Tastatureingaben, oder Systemereignisse, wie zum Beispiel ungenügender Speicher, sein.
Fehlalarm	Erscheint, wenn ein Virenscanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist. Kann bei heuristischem Virenprüfen auftreten.
Heuristisch	Eine Methode, um neue Viren zu identifizieren. Diese Prüfmethode beruht nicht auf spezifische Virussignaturen. Der Vorteil einer heuristischen Prüfung ist, dass man nicht von einer neuen Virusvariante getäuscht werden kann. Manchmal kann auch ein verdächtiger Code in einem normalen Programm gemeldet werden, indem das so genannte Fehlalarm generiert wird.
IP	Internet Protocol - Das TCP/IP Protokol ist verantwortlich für die korrekte IP Adressierung und die korrekte Zustellung der Datenpakete.
Java applet	Ein Java Programm, das nur auf Webseiten läuft. Um ein Applet auf einer Webseite zu benutzen, gibt man den Namen und die Grösse (Länge und Breite- in Pixel) des Applets an. Wenn die Webseite abgerufen wird, lädt der Browser das Applet vom Server herunter und führt es auf der Benutzermaschine (dem Client) aus. Applets sind keine Anwendungen, da sie von strengen Sicherheitsprotokollen gesteuert werden. Obwohl Applets auf dem Client laufen, können diese keine Daten auf der Clientmaschine lesen oder schreiben. Zusätzlich sind die Applets weiter begrenzt, so dass sie nur Daten aus

der Domäne lesen und beschreiben können, die sie unterstützen.

Komprimierte Programme

Eine Datei in einem komprimierten Format. Viele Betriebssysteme und Anwendungen enthalten Befehle, die das Komprimieren einer Datei ermöglichen, so dass diese weniger Speicherplatz benötigt. Zum Beispiel: Angenommen Sie haben einen Text, der 10 aufeinander folgende Leerzeichen enthält. Normalerweise nehmen diese 10 Bytes Speicherplatz ein.

Ein Programm, das Dateien komprimiert, würde die Leerzeichen durch ein spezielles Zeichen Leerzeichenreihe ersetzen, gefolgt von der Zahl der Leerzeichen, die ersetzt wurden. In diesem Fall sind nur noch zwei Bytes notwendig statt zehn. Das wäre ein Beispiel für eine Komprimierungstechnik, es gibt aber noch viele andere.

Laufwerk

Ein Gerät, das rotierende Speichermedien lesen und beschreiben kann.

Ein Festplatten-Laufwerk liest und beschreibt Festplatten.

Ein Disketten-Laufwerk liest und beschreibt Disketten.

Laufwerke können sowohl interner (im Rechner eingebaut) als auch externer (in einem Gehäuse, das an den Rechner angeschlossen wird) Art sein.

Logdatei (Berichtdatei)

Eine Datei, die stattgefundene Aktivitäten aufzeichnet. Zum Beispiel speichert BitDefender eine Logdatei mit den geprüften Pfaden, Ordnern und der Archivanzahl, aber auch den geprüften, infizierten oder verdächtigen Dateien.

Mail client

Ein E-Mail Client ist eine Anwendung, die das Senden und Empfangen von E-Mails ermöglicht.

Makrovirus

Eine Virusform, die in einem Dokument als eingebettetes Makro verschlüsselt wird. Viele Anwendungen, wie Microsoft Word und Excel, unterstützen mächtige Makrosprachen.

Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Doku-

ments ausgeführt wird. Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.

Nicht heuristisch

Diese Prüfmethode beruht auf einer spezifischen Virussignatur. Der Vorteil einer nicht heuristischen Prüfung ist, dass diese nicht von einem Scheinvirus getäuscht werden kann, und dass dieser keinen falschen Alarm auslöst.

Phishing

Dabei wird eine E-Mail mit einer betrügerlichen Absicht an einen Nutzer gesendet. Der Inhalt dieser E-Mail gibt vor, von einem bekannten und serös arbeitenden Unternehmen zu stammen. Zweck dieser E-Mail ist es dann, private und geheime Nutzerdaten preiszugeben, worauf der Absender beabsichtigt, die Identität des Nutzers anzunehmen. Die E-Mail führt den Benutzer dann auf eine Webseite, in der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TAN's oder PIN's preiszugeben. Dies soll auch Gründen der Aktualisierung geschehen. Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

Pfad

Zeigt die Stelle an, an der sich eine Datei in einem Rechner befindet. Diese Pfadangaben enthalten gewöhnlich den hierarchischen Aufbau des Dateiverzeichnisses: Laufwerke, Ordner, Unterverzeichnisse, die Datei und ihre Erweiterung.

Der Weg zwischen zwei Punkten, wie zum Beispiel der Kommunikationskanal zwischen zwei Rechnern.

Polymorpher Virus

Ein Virus, der seine Form mit jeder Datei, die er infiziert, ändert. Da diese Viren kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

Schnittstelle

Stelle eines Rechners, an die ein Gerät angeschlossen werden kann. Rechner haben verschiedenartige Schnittstellen. Intern gibt es Schnittstellen zum Anschluss von Festplatten, Grafikkarten und Tastaturen. Extern haben Rechner Schnittstellen zum Anschluss von Modems, Druckern und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen. Die Schnittstellennummer gibt die Art der Schnittstelle an. Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

Skript

Ein anderer Begriff für Makro - oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

Spam

Junk-E-Mail oder Junk-Postings in Newsgroups. Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

Spyware

Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten überwacht und über seine Internetverbindung abruft. Dies geschieht in der Regel zu Werbezwecken. Typischerweise werden Spyware-Anwendungen als verborgene Komponente in Freeware- oder Sharewareprogrammen gebündelt, die aus dem Internet heruntergeladen werden können. Es ist jedoch darauf hinzuweisen, dass die Mehrzahl der Shareware- und Freeware-Anwendungen frei von Spyware ist. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und übertragt diese Daten im Hintergrund am jemand anderen. Spyware kann auch Informationen über E-Mail-Adressen und sogar Kennwörter und Kreditkartennummern sammeln.

Einem Trojanischen Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren. Eine weit verbreitete Möglichkeit, ein Opfer von Spyware zu werden, ist der Download von bestimmten heute erhältlichen Peer-to-Peer-Dateitauschprogrammen (Direktverbindungen von Computern).

Abgesehen von den Fragen der Ethik und des Datenschutzes bestiehlt Spyware den Anwender, indem sie Speicherressourcen seines Rechners nutzt und den Internetzugriff verlangsamt, indem über seine Internetverbindung Informationen an den Spyware-Heimatserver gesendet werden. Da Spyware Speicher und Systemressourcen verbraucht, können die im

	Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.
Startup Objekt (Autostart-Objekt)	Jede Datei, die sich in diesem Ordner befindet, öffnet sich, wenn der Rechner gestartet wird. Zum Beispiel ein Startbildschirm, eine Sounddatei, die abgespielt wird, wenn der Rechner gestartet wird, ein Erinnerungskalender oder Anwendungsprogramme können Autostart-Objekte sein. Gewöhnlich wird eine Alias-Datei (Verknüpfung) statt der eigentlichen Datei in diesen Ordner gelegt.
System tray	Der System Tray wurde mit Windows 95 eingeführt und befindet sich auf der Windows Taskleiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Er enthält kleine Icons zur Information und zum leichteren Zugriff, zum Beispiel: Fax, Drucker, Modem, Lautstärke und mehr. Um auf die Details und Steuerungen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.
TCP/IP	Transmission Control Protocol/Internet Protocol - Im Internet werden eine Vielzahl von verschiedener Hardware und Betriebssystemen miteinander verbunden. Das TCP/IP Protokoll bietet eine Möglichkeit all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.
Trojaner	Ein vernichtendes Programm, das sich als eine freundliche Anwendung tarnt und auftritt. Im Unterschied zu Viren vervielfältigen sich die Trojaner (auch "trojanische Pferde" genannt) nicht, aber sie können zerstörerisch sein. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Viren zu befreien, stattdessen aber den Rechner infiziert. Viele Trojaner öffnen den Rechner für den Zugriff von aussen. Der Begriff entstammt einer Geschichte in Homer's "Ilias", in der die Griechen Ihren Feinden, den Trojanern, angeblich als Sühnegabe ein hölzernes Pferd schenken. Aber, nachdem die Trojaner das Pferd innerhalb der Stadtmauern gebracht hatten, schlichen die Soldaten aus der Bauchhöhle des Pferdes, öffneten sie die Tore der Stadt und ermöglichten somit

	ihren Landsmännern einzudringen und auf diese Weise Troja zu besetzen.
Update (Aktualisierung)	Neue Softwareversionen oder Hardwareprodukte, die eine ältere Version ersetzen. Die Update-Installationsroutine sucht nach älteren Versionen auf dem Rechner, da sonst kein Update installiert werden kann. BitDefender hat sein eigenes Update Modul, welches das manuelle oder automatische Prüfen nach Updates ermöglicht.
Virus	Ein Programm oder ein Codestück, das auf einen Rechner geladen wird, ohne dass der Benutzer Kenntnis davon hat und welches sich allein ausführt. Die Resultate von Viren können einfache Scherzmeldungen aber auch die Zerstörung von Hardware sein. Die meisten Viren können sich selber vervielfältigen. Alle Computerviren sind von Menschenhand geschrieben. Ein Virus, der sich immer wieder vervielfältigen kann ist sehr einfach zu schreiben. Sogar ein solch einfacher Virus ist fähig sich durch Netzwerke zu verschicken und Sicherheitssysteme zu überbrücken.
Virusdefinition	Ein binäres Virusmuster, das von einem Antivirus Programm verwendet wird, um einen Virus zu entdecken und zu entfernen.
Wurm	Ein Programm, das sich über ein Netzwerk verbreitet. Es kann sich nicht an andere Programme anhängen.